NIST Special Publication 800-128

Guide for Security Configuration Management of Information Systems

Arnold Johnson
Kelley Dempsey
Ron Ross
Sarbari Gupta
Dennis Bailey

INFORMATION SECURITY

INITIAL PUBLIC DRAFT

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

March 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in Circular A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in Circular A-130, Appendix III.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

Draft NIST Special Publication 800-128, 70 pages

(March 2010)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic mail: sec-cert@nist.gov

Compliance with NIST Standards and Guidelines

In accordance with the provisions of FISMA,[1] the Secretary of Commerce shall, on the basis of standards and guidelines developed by NIST, prescribe standards and guidelines pertaining to federal information systems. The Secretary shall make standards compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of operation or security of federal information systems. Standards prescribed shall include information security standards that provide minimum information security requirements and are otherwise necessary to improve the security of federal information and information systems.

- Federal Information Processing Standards (FIPS) are approved by the Secretary of Commerce and issued by NIST in accordance with FISMA. FIPS are compulsory and binding for federal agencies.[2] FISMA requires that federal agencies comply with these standards, and therefore, agencies may not waive their use.
- Special Publications (SPs) are developed and issued by NIST as recommendations and guidance documents. For other than national security programs and systems, federal agencies must follow those NIST Special Publications mandated in a Federal Information Processing Standard. FIPS 200 mandates the use of Special Publication 800-53, as amended. In addition, OMB policies (including OMB Reporting Instructions for FISMA and Agency Privacy Management), state that for other than national security programs and systems, federal agencies must follow certain specific NIST Special Publications.[3]
- Other security-related publications, including interagency reports (NISTIRs) and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when specified by OMB.
- Compliance schedules for NIST security standards and guidelines are established by OMB in policies, directives, or memoranda (e.g., annual FISMA Reporting Guidance).

[1] The E-Government Act (P.L. 107-347) recognizes the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

[2] The term *agency* is used in this publication in lieu of the more general term *organization* only in those circumstances where its usage is directly related to other source documents such as federal legislation or policy.

[3] While federal agencies are required to follow certain specific NIST Special Publications in accordance with OMB policy, there is flexibility in how agencies apply the guidance. Federal agencies should apply the security concepts and principles articulated in the NIST Special Publications in accordance with and in the context of the agency’s missions, business functions, and environment of operation. Consequently, the application of NIST guidance by federal agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems. Given the high priority of information sharing and transparency with the federal government, agencies also consider reciprocity in developing their information security solutions. When assessing federal agency compliance with NIST Special Publications, Inspectors General, evaluators, auditors, and assessors, should consider the intent of the security concepts and principles articulated within the specific guidance document and how the agency applied the guidance in the context of its mission/business responsibilities, operational environment, and unique organizational conditions.

Acknowledgments

The authors, Arnold Johnson, Kelley Dempsey, and Ron Ross of NIST, and Sarbari Gupta and Dennis Bailey of Electrosoft, wish to thank their colleagues who reviewed drafts of this document and contributed to its development. A special note of thanks goes to Peggy Himes and Liz Lennon for their superb technical editing and administrative support, and to Murugiah Souppaya, Karen Scarfone, and Blair Heiserman, for their review of the document and their insightful recommendations.

Additional acknowledgments will be added to the final version of the publication.

Table of Contents

CHAPTER ONE

INTRODUCTION

THE NEED FOR SECURITY CONFIGURATION MANAGEMENT TO PROTECT INFORMATION AND INFORMATION SYSTEMS

An information system is composed of many components[4] that can be interconnected in a multitude of arrangements to meet a variety of business, mission, and information security needs. How these information system components are networked, configured, and managed is critical in providing adequate information security, and supporting an organization's risk management process.

An information system is typically in a constant state of change in response to new or enhanced hardware and software capability, patches for correcting errors to existing components, new security threats, and changing business functions, etc. Implementing information system changes almost always results in some adjustment to the system baseline configuration. To ensure that the required adjustments to the system configuration do not adversely affect the information system security, a well-defined security configuration management process is needed.

1.1 PURPOSE AND APPLICABILITY

FISMA requires agencies to establish "minimally acceptable system configuration requirements" within their information security program, and NIST SP 800-53 defines a set of security controls which support this requirement.

The Configuration Management family of controls from NIST SP 800-53 (CM-1 through CM-9) are related to the configuration management of information systems within an organization. The purpose of this publication is to elaborate on the application of these security controls and provide guidelines for managing the configuration of the information system architecture and associated components for secure processing, storing, and transmitting of information in the information environment. Security configuration management provides an important function for establishing and maintaining secure information system configurations, and provides important support for managing risks in information systems.

The guidelines in this special publication are applicable to all federal information systems[5] other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542. State, local, and tribal governments, as well as private sector organizations, are encouraged to consider using these guidelines, as appropriate.

This security configuration management publication is intended to provide guidelines for organizations responsible for managing and administrating the security of federal information system computing environments. For organizations responsible for the security of information processed, stored, and transmitted by external or service-oriented computing environments (e.g., cloud computing environment providers), the security configuration management concepts and

[4] Information system components include, for example, mainframes, workstations, servers (e.g., database, electronic mail, authentication, Web, proxy, file, domain name), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.

[5] A federal information system is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

principles presented here can aid organizations in establishing assurance requirements for suppliers providing external computing services.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse audience of information system and information security professionals including:

- Individuals with information system and information security management and oversight responsibilities (e.g., chief information officers, senior agency information security officers, and authorizing officials);

- Individuals with information system development responsibilities (e.g., program and project managers, mission/application owners, system designers, system and application programmers);

- Individuals with information security implementation and operational responsibilities (e.g., information system owners, information owners, information system administrators, information system security officers); and

- Individuals with information system and information security assessment and monitoring responsibilities (e.g., auditors, Inspectors General, assessors/assessment teams).

Commercial companies producing information technology products and systems, creating information security-related technologies, and providing information security services can also benefit from the information in this publication.

1.3 RELATIONSHIP TO OTHER SECURITY PUBLICATIONS

Security configuration management concepts and principles described in this publication provide supporting information for NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, primarily, the Configuration Management family of security controls and other security controls that draw upon configuration management activities in implementing those controls. This publication also provides important supporting information for the Monitor Step (Step 6) of the Risk Management Framework that is discussed in NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, and NIST SP 800-39 *Managing Risk from Information Systems: An Organizational Perspective* (Second Public Draft).

This publication often refers to information from NIST SP 800-70, Revision 1, *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*; NIST SP 800-117, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP)*; and NIST SP 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP), Version 1.0,* as a potential means of automated support in conducting many configuration management activities.

Additionally, this publication refers to numerous special publications that provide guidance on use and configuration of specific technologies for securing information systems. Many of these publications are identified in Appendix F, Best Practices for Establishing Secure Configurations.

1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with security configuration management including: (i) an overview of generic configuration management versus information technology (IT) security configuration management of information systems; (ii) the major phases of security configuration management; (iii) the fundamental concepts relevant to the practice of security configuration management; and (iv) the primary roles and responsibilities relevant to security configuration management.

- **Chapter Three** describes the process of applying security configuration management practices to information systems within an organization including: (i) planning security configuration management activities for the organization; (ii) configuring the information system to a secure state; (iii) maintaining the configuration of the information system in a secure state; (iv) monitoring the configuration of the information system to ensure that the configuration is not inadvertently altered from its approved state; and (v) the use of standardized Security Content Automation Protocol (SCAP) protocols for supporting automated tools in verifying information system configurations.

- **Supporting appendices** provide more detailed security configuration management information including: (i) general references; (ii) glossary of terms and definitions; (iii) acronyms; (iv) sample configuration management plan template; (v) sample configuration change request template; (vi) best practices for establishing secure configurations in information systems, and (vii) flow charts for various Security Configuration Management (SCM) processes and activities.

CHAPTER TWO

THE FUNDAMENTALS

BASIC CONCEPTS OF SECURITY CONFIGURATION MANAGEMENT

This chapter presents the basic concepts of security configuration management including: (i) an overview of configuration management; (ii) the primary phases of security configuration management; (iii) security configuration management concepts; and (iv) the roles and responsibilities relevant to security configuration management.

2.1 OVERVIEW

This section provides an overview of configuration management including its importance in managing organizational risks from information systems, the basic terms associated with configuration management, and characterization of information system security configuration management within the configuration management discipline.

2.1.1 THE CHALLENGE OF PROTECTING INFORMATION AND MANAGING RISK

As the ubiquity of information technology increases the dependence on information systems, organizations are faced with an increase in the number and severity of threats that can have adverse impacts on operations, assets, and individuals. Given the potential for harm that can arise from environmental disruptions, human errors, and purposeful attacks by hostile entities and other threats, an organization must place greater emphasis on the management of risk associated with information systems as it attempts to carry out its mission and business processes. The cornerstone of any effort to manage organizational risk related to information systems is an effective information security[6] program. Title III of the E-Government Act of 2002 known as the Federal Information Security Management Act (FISMA) was developed to provide a broad framework for information security programs within the federal government.

While FISMA outlines a comprehensive structure for establishing an information security program, it is incumbent upon the organization to implement its directives in a manner that provides adequate security[7] for protecting information and information systems. As threats continue to evolve in an environment where organizations have finite resources with which to protect themselves, security has become a risk-based activity where the operational and economic costs of ensuring that a particular threat is not exercised must be balanced against the needs of the organization's mission and business processes. In a world of limited resources, the practice of risk management is fundamental to an information security program.

In risk-based mission protection strategies, organizations must explicitly identify, mitigate and accept risks associated with the use of information systems in carrying out missions and business processes. Careful consideration must be given to how a range of diverse threats can expose existing vulnerabilities and cause harm to the organization. In the management of risk, organizations often have very little control over the threat side of the equation. Earthquakes,

[6] Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability [44 U.S.C., Sec. 3542]. For the purposes of this publication, "security" is used synonymously with "information security."

[7] Adequate security is security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

floods, disgruntled employees, hackers, and other threats do not lend themselves to management by the organization. It is the vulnerability side of the equation where organizations can have the most impact when it comes to risk management. Vulnerabilities represent the various types of weaknesses in an information environment[8] that can be exercised by a threat.[9] While an analysis of information system vulnerabilities reveals a variety of potential causes, many vulnerabilities can be traced to software flaws and improper configurations[10] [11] of information system components.

The management of configurations in an information environment has traditionally been viewed as an IT management best practice.[12] Using configuration management to gain greater control over and ensure the integrity of IT resources facilitates asset management, improves incident response, help desk, disaster recovery and problem solving, aids in software development and release management, enables greater automation of processes, and supports compliance with policies and preparation for audits.

2.1.2 CONFIGURATION MANAGEMENT BASICS

Configuration management has been applied to a broad range of products and systems in subject areas such as automobiles, pharmaceuticals, and information systems. Some basic terms generally associated with the configuration management discipline are briefly explained below.

Configuration Management (CM) comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems. The practice of configuration management is implemented through the establishment of the baseline configuration.

A *Configuration Item (CI)* is an identifiable part of a system that is a discrete target of configuration control processes.

A *Baseline Configuration* is a set of specifications for a system, or CI within a system, that has been formally reviewed and agreed on at a point in time, and which can be changed only through change control procedures.

[8] An information environment is an aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself [CNSS Inst. 4009]. When *information environment* is used within this publication, it refers to the information system components that interface/interact with the enterprise-wide information technology infrastructure. It is also used to indicate multiple information systems.

[9] A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [CNSS Inst. 4009, Adapted]. Vulnerabilities are sometimes referred to more narrowly, for example, as mistakes in software (see Common Vulnerabilities and Exposures). In this publication, the broader CNSS definition is used with the addition of misconfigurations as an example of a vulnerability.

[10] A configuration is the possible conditions in which an information system or system component can be arranged that affect the security posture of the information system. There are a large number of configurations that can impact an information system including configuration settings, security controls, physical and logical placement, software loads, and patch levels.

[11] Improper configuration of an information system or system component that leads to a vulnerability being exposed.

[12] Best practices are often considered to be proven practices or processes that have been successfully used by multiple organizations. IT management best practices, as referred to in this publication, are viewed from an organization-wide perspective as practices that best support the mission and business functions or services of the organization.

A *Configuration Management Plan* (CM Plan) is a comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems. The basic parts of a CM Plan include:

- Configuration *Change Control Board* – charter and organizational structure (roles and responsibilities) of the body of personnel responsible for CM;
- Configuration Item *Identification* – methodology for selection and naming of configuration items that need to be placed under CM;
- *Baseline Configuration Management* – process for the establishment and management of the baseline configuration for the identified configuration items;
- Configuration *Change Control* – process for managing updates to the baselines for the configuration items; and
- Configuration *Monitoring* – process for assessing or testing the level of compliance with the established configuration baseline and mechanisms for reporting on the configuration status of items placed under CM.

This guideline is associated with the application of configuration management practices as it applies to information systems. The configuration of an information system is a representation of the system's components, how each component is configured, and how the components are connected or arranged to implement the information system. The activities involved in managing the configuration of an information system include development of a configuration management plan, establishment of a configuration change control board, development of a methodology for configuration item identification, establishment of the baseline configuration, development of a configuration change control process, and development of a process for configuration monitoring and reporting.

2.1.3 SECURITY CONFIGURATION MANAGEMENT[13]

The configuration of an information system and its components has a direct impact on the security posture (i.e., official position regarding the ability to protect the confidentiality, integrity, and availability of information stored, processed, or transmitted) of the system. How those configurations are established and maintained requires a disciplined approach for providing adequate security. Changes to the configuration of an information system are often needed to stay up to date with changing business functions and services, and information security needs. These changes can adversely impact the previously established security posture; therefore, effective configuration management is vital to the establishment and maintenance of security of information and the information system.

[13] There are a number of organizations that have documented best practice standards and guidelines for configuration management which precede this Special Publication and influence its direction including: The American National Standards Institute (ANSI)/ International Organization for Standardization (ISO) ISO 10007:2003; the Institute of Electrical and Electronic Engineers (IEEE) (Standard 1042-1987); the Capability Maturity Model Integration (CMMI) with their focus on configuration management for software development documents (http://www.sei.cmu.edu/legacy/scm/); the Information Technology Infrastructure Library (ITIL) for its influence on the integration of configuration within information technology management (http://www.itil-officialsite.com/home/home.asp); and the International Organization for Standardization (ISO) for its attention to configuration management within quality management systems.

Security Configuration Management (SCM) is the management and control of configurations for an information system with the goal of enabling security and managing risk. SCM applies the general concepts, processes, and activities of CM but with a focus on outcomes that affect the security posture of the information system.

SCM should be integrated into any similar configuration management activities that may be in place for the information system. Integration into an overall CM program would include SCM activities such as identification and recording of configurations that impact the security posture of the information system, the consideration of security risks in approving the initial configuration, and the analysis of security implications of proposed changes to the information system configuration.

A large part of the effort with implementing a SCM program is in getting it off the ground. There may be an initial investment in planning and developing a program that is comprehensive enough to span multiple technologies, organization divisions, and disparate processes, and can deliver consistent results while supporting the organization's missions and business processes. After policy and planning, tools must be procured and implemented, system components inventoried and documented, and processes reengineered to account for new ways of managing technology that have an eye toward secure configurations.

Once in place, SCM requires an ongoing investment in time and resources. A flood of patches, security fixes, and updates require time for impact analysis, and a growing volume of malware (viruses, Trojans, etc.) leave little room for delay. As changes to information systems are made, baseline configurations should be updated, specific configuration settings confirmed, and configuration items tracked, verified and reported. SCM is a continuous activity that, once incorporated into normal IT management processes, touches all stages of the system development life cycle (SDLC). Organizations that implement SCM throughout the SDLC and make its tenets a part of the IT management culture are most likely to reap its fruits in terms of the improvement of security and more effective management of organizational risk.

The remainder of this publication focuses on the integration of information system security with information system configuration management.

The terms *configuration management* and *security configuration management*, and the abbreviations CM and SCM, will be used interchangeably to refer to configuration management practices that are focused on the security posture of information systems.

2.2 THE PHASES OF SECURITY CONFIGURATION MANAGEMENT

Security configuration management of information systems involves a set of activities that can be organized into four major phases – Planning, Configuring to a Secure State, Maintaining Secure State, and Monitoring. It is through these phases that SCM not only enables security for an information system and its components, but also supports the management of organizational risk. Chapter 3 presents the detailed processes and considerations in implementing the SCM activities in each of these phases.

The four phases of SCM are illustrated in Figure 1 and described below.

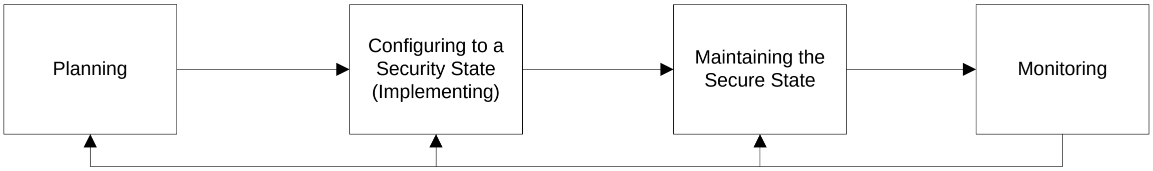

Planning
Configuring to a Security State (Implementing)
Maintaining the Secure State
Monitoring

Figure 1 - Security Configuration Management Phases

2.2.1 PLANNING

As with many security activities, planning can greatly impact the success or failure of the effort. As a part of planning, the scope or applicability of SCM processes should be identified.

Planning includes developing policy to incorporate SCM into existing information technology and security programs, and then disseminating the policy throughout the organization. Policy should address areas such as the implementation of SCM plans, Change Control Boards (CCBs), configuration change control processes, tools, and technology, the use of secure configuration standards[14] and baseline configurations, monitoring, and metrics for compliance with established SCM policy and standards to reinforce the significance of SCM.

2.2.2 CONFIGURING TO A SECURE STATE

After the planning and preparation activities are completed, a secure baseline for the information system is developed, reviewed, approved, and implemented. The approved baseline configuration for an information system and associated components represent the most secure state consistent with operational requirements and constraints. For a typical information system, the secure baseline may include such things as configuration settings, software loads, patch levels, how the information system is physically or logically arranged, and how various security controls are implemented. Where possible, automation should be used to provide a uniform mechanism to implement the baseline configurations across the information system.

2.2.3 MAINTAINING SECURE STATE

Given the continually evolving nature of an information system and the mission it supports, the challenge for organizations is not only to find an initial baseline configuration that represents a secure state, (which is also cost-effective and supports important mission and business processes), but also to maintain that secure state in the face of the significant waves of change that ripple through organizations.

In this phase of SCM, the emphasis is put on the management of change to maintain the security state of the information system. Through the use of SCM practices, organizations can ensure that all changes are formally proposed, reviewed, and approved prior to implementation. As part of the change control effort, organizations can employ a variety of access restrictions for change including access controls, process automation, abstract layers, change windows, and verification

[14] An established benchmark (e.g., NIST checklists, DISA STIGs, etc.) that stipulates specific secure configuration settings for a given IT platform.

and audit activities to limit the chances of unauthorized changes finding their way into the information system.

2.2.4 MONITORING

Monitoring activities are used as the mechanism within SCM to validate that the information system is configured to a secure baseline state as intended. Planning and implementing secure configurations and then controlling change is not always sufficient to ensure that an information system which was once secure will remain secure. Monitoring identifies undiscovered system components, misconfigurations, vulnerabilities, and unauthorized changes, all of which, if not addressed, can expose organizations to increased risk. Using automated tools helps organizations to identify when the information system is not in compliance with the established baseline and when remediation actions are necessary. In addition, the use of automated tools facilitates the documentation of deviations from the baseline.

Monitoring is done through assessment and reporting activities. SCM reports address the security state of individual information systems and can be used to support the Risk Management Framework continuous monitoring requirements. Monitoring can also support gathering of information for metrics that can be used to provide quantitative evidence that the SCM program is meeting its stated goals, and can be used to improve SCM processes.

2.3 SECURITY CONFIGURATION MANAGEMENT CONCEPTS

This section describes the fundamental concepts relevant to the practice of SCM within an organization. Recognizing that organizations have widely varying missions and organizational structures, there may be differences in the way that SCM is implemented and managed.

2.3.1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

The development of documented SCM policy communicates senior management’s expectations for SCM to members of the organization through specific, measurable, and confirmable objectives. It is a top-down approach which defines what is required and what is not permitted with respect to using SCM to manage and control information resources.

While policy defines the objectives for what must be done, procedures describe how the policy objectives can be met through specific actions and results. SCM procedures are developed to describe the methodology and tasks for each activity that supports implementation of the SCM policy.

Documenting of configuration management policy and procedures is performed during the Planning phase of SCM and supports the implementation of NIST SP 800-53 control **CM-1 Configuration Management Policy and Procedures**.

2.3.2 CONFIGURATION MANAGEMENT PLAN

The Configuration Management Plan serves to describe how SCM policy will be implemented. The SCM Plan could be written to apply to an entire organization, or it can be localized and tailored to an information system or a group of information systems within the information environment. The SCM Plan may take the form of an all-inclusive, stand-alone document that describes all aspects of SCM or may be contained within SCM procedures. An SCM Plan may also take the form of a hierarchical set of documents and appendices that taken together describe all aspects of SCM. Finally, the SCM Plan may take the form of a set of predefined data elements in a repository. Personnel who are responsible for managing and/or monitoring the configuration of the information system(s) use the SCM Plan.

The SCM Plan is produced during the Planning phase and supports the implementation of NIST SP 800-53 control **CM-1 Configuration Management Policy and Procedures.** The SCM Plan also supports the implementation of NIST SP 800-53 control **CM-9 Configuration Management Plan**.

2.3.3 CHANGE CONTROL BOARD

The Change Control Board (CCB) is a group typically consisting of two or more individuals that have the collective responsibility and authority to review and approve proposed changes to an information system. The group, which should represent various perspectives from within the organization, is chosen to evaluate and approve changes to the information system. The CCB acts as a check and balance on configuration change activity, assuring that proposed changes are held to organizationally defined criteria (e.g., scope, cost, impact on security) before being implemented.

The CCB may be less formal for information systems which have limited size, scope, and criticality in the context of the mission of the organization. The organization determines the size and formality of the CCB that is appropriate for a given information system within the organization.

The CCB establishment is part of the Planning phase of SCM and supports the implementation of NIST SP 800-53 control **CM-3 Configuration Change Control.**

2.3.4 INFORMATION SYSTEM (IS) COMPONENT INVENTORY

The IS component inventory is a list of the physically identifiable components within an information system. A consolidated representation of the IS components within all of the information systems within an organization allows the organization to have greater visibility into and control over its information environment, facilitating the implementation, operation, and management of a security program. The organization determines the level of granularity required for tracking the IS components for SCM. For example, one organization may track a workstation (with all peripherals) as a single component while another may document each peripheral as a separate component in the inventory.

Each IS component should be associated with only one information system and the authority over and responsibility for each IS component should be with only one information system owner (i.e., every item in the IS component inventory should fall within the authorization boundary of a single information system).

Creating an inventory of IS components for an information system is part of the Planning phase of SCM and supports the implementation of the NIST SP 800-53 control **CM-8 Information System Component Inventory.**

2.3.5 CONFIGURATION ITEMS

In the context of SCM of information systems, a *configuration item* (CI) is an identified part of an information system whose configuration is managed as part of the SCM program. This implies that the CI is identified, labeled, and tracked during its life cycle – the CI is the target of many of the activities within SCM, such as configuration change control and monitoring activities. A CI may be a specific information system component (e.g., server, workstation, router), a group of information system components (e.g., group of servers with like operating systems, group of network components such as routers and switches), a non-component entity (e.g., software such as a Web application, firmware, documentation), or an information system as a whole. CIs give organizations a way to decompose the information system into manageable parts whose configurations can be actively managed.

The purpose of breaking up an information system into two or more CIs is to allow more granularity and control in managing the secure configuration of the system. The level of granularity will vary among organizations and systems and should be balanced against the associated management overhead for each CI. In one organization, it may be appropriate to create a single CI to track all of the laptops within a system while in another organization, each laptop may represent an individual CI.

Identification of the configuration items that compose an information system is part of the Planning phase of SCM and supports the implementation of NIST SP 800-53 control **CM-3 Configuration Change Control.**

2.3.6 SECURE CONFIGURATIONS OF INFORMATION SYSTEMS

Configurations represent the possible conditions in which an information system and its components can be arranged. Secure configurations are designed to reduce the organizational security risk from operation of an information system, and may involve using trusted or approved software loads, maintaining up-to-date patch levels, applying secure configuration settings of the IT products used, and implementation of endpoint protection platforms. Secure configurations for an information system are most often achieved through the application of secure configuration settings to the IT products (e.g., operating systems, databases, etc.) used to build the information system. For example, a secure configuration for selected IT products used within the information system or organization could incorporate the principle of least functionality. Least functionality helps to minimize the potential for introduction of security vulnerabilities and includes, but is not limited to, disabling or uninstalling unused/unnecessary operating system (OS) functionality, protocols, ports, and services, and limiting the software that can be installed and the functionality of that software.

Implementing secure configurations is part of the Configure to Secure State phase of SCM and supports the implementation of NIST SP 800-53 controls **CM-6 Configuration Settings** and **CM-7 Least Functionality.**

2.3.7 BASELINE CONFIGURATION

A baseline configuration is a well-defined, documented, and approved specification to which an information system is built. It describes the approved configuration of an information system including all its hardware, software, and firmware components, how the components are interconnected, and the physical and logical locations of each. In the context of SCM, a baseline configuration is a collection of formally approved configuration state(s) of one or more CI(s) that compose the information system. The baseline configuration is used for information system restore and serves as the basis against which the next change or set of changes to the information system is made.

The baseline configuration of an information system may evolve over time depending on the stage of the system development life cycle (SDLC). Early in the SDLC when an information system is being initiated and acquired, a baseline may be a set of functional requirements. As the information system is developed and implemented, the baseline will expand to include the technical design, the software load, the architecture, and configuration of the information system and its individual components. A baseline configuration may also represent different information computing environments such as development, test, and production.

When a new baseline configuration is established, the implication is that all of the changes from the last baseline have been approved. Older versions of approved baseline configurations should be maintained and made available for review or rollback as needed.

Developing and documenting the baseline configuration for an information system is part of the Configuring to a Secure State phase of SCM and supports the implementation of NIST SP 800-53 control **CM-2 Baseline Configuration.**

2.3.8 CONFIGURATION CHANGE CONTROL

Configuration change control is the documented process for managing and controlling changes to the configuration of an information system or its constituent CIs. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control is applied to include changes to components of the information system, changes to the configuration settings for information technology products, emergency/unscheduled changes, and changes to remediate flaws. Changes are controlled from the time the change is proposed to the implementation and testing of the change. Each step in the change process is clearly articulated along with the responsibilities and authorities of the roles involved.

Configuration change control falls under the Maintaining Secure State phase of SCM and supports the implementation of NIST SP 800-53 control **CM-3 Configuration Change Control** and **CM-5 Access Restrictions for Change**.

2.3.9 SECURITY IMPACT ANALYSIS

Security impact analysis is the deliberate consideration of the impact of a change on the security state of the information system. Because information systems are typically in a constant state of change, it is important to understand the impact of changes on the functionality of existing security controls. Security impact analysis should be incorporated into the documented configuration change control process.

The analysis of the security impact of a change occurs in two phases. The first is when proposed changes are analyzed and evaluated for adverse impact on security before they are approved. Once the changes are implemented and tested, the second phase of security impact analysis is performed to ensure that the changes have been implemented as approved, and to determine if there are any unanticipated effects of the change on existing security controls.

Security impact analysis is performed as a part of the Maintaining Secure State phase of SCM and supports the implementation of NIST SP 800-53 control **CM-4 Security Impact Analysis.**

2.3.10 CONFIGURATION MONITORING

Configuration monitoring involves activities to determine whether information systems are configured in accordance with the organization’s approved baseline configurations, and that the

IS components identified within the information system match the IS component inventory being maintained by the organization.

Configuration monitoring also helps to enforce the policies and procedures of SCM. Configuration monitoring motivates staff members to perform SCM activities in accordance with SCM policies and procedures. Configuration monitoring also supports organizations in their efforts to remain compliant with FISMA and other security compliance frameworks. Information gathered during configuration monitoring can be used to support continuous monitoring activities including ongoing assessments of specific security controls, and updates to security documentation such as System Security Plans, Security Assessment Reports, and Security Status Reports.

Configuration compliance activities are an important part of the Monitoring phase of SCM and support the implementation of **all NIST SP 800-53 controls in the CM Family**.

2.4 SCM ROLES AND RESPONSIBILITIES

The set of roles (at the organizational as well as the information system level) that is relevant to the SCM program should be defined along with the responsibilities. Typically, the following roles and responsibilities with respect to SCM include:

Senior Agency Information Security Officer (SAISO)
The SAISO provides organization-wide procedures and/or templates for SCM, manages or participates in the Change Control Board, and/or provides technical staff for security impact analyses. Organizations may also refer to this position as the Senior Information Security Officer (SISO) or the Chief Information Security Officer (CISO).

Information System Owner (ISO)
The information system owner identifies, defines, and ensures implementation of the aspects of SCM for the information system that have not been defined by the organization of which the information system is a part.

Information System Security Officer (ISSO)
The ISSO assists the information system owner with implementation of SCM for the system, conducts configuration monitoring activities (reporting and analysis), and may sit on the CCB.

Information System Administrator (ISA)
The information system administrator implements approved secure baseline configurations, incorporates secure configuration settings for IT products, and conducts/assists with configuration monitoring activities as needed. In addition, the system administrator should be included in the process for determining the appropriate baseline for each CI.

Information System User (ISU)
The information system user initiates change requests, assists with functional testing, and complies with SCM requirements.

CHAPTER THREE

THE PROCESS

IMPLEMENTATION AND APPLICATION OF SECURITY CONFIGURATION MANAGEMENT

This chapter describes the process of applying security configuration management to information systems within an organization. The goal of SCM activities is to manage and monitor the configurations of information systems to achieve adequate security and minimize organizational risk while providing the desired business functionality and services. A typical SCM implementation comprises some activities that are performed centrally by the organization and additional activities that are performed by each information system owner.

The following sections discuss SCM activities that occur within each of the four phases of SCM. Some of these activities are generally more efficiently performed centrally, and other activities are generally performed locally for each information system. Each organization should determine what activities should be done centrally and what activities should be done by each information system owner in accordance with organizational mission requirements. Appendix G provides flow charts of various SCM activities described here. The flow charts are intended to serve as examples for organizations to draw upon for developing their own organizational and information system SCM processes.

3.1 PLANNING

This section focuses on activities in the Planning phase of security configuration management. The section describes various SCM planning activities and suggests some implementation approaches to assist organizations in developing security configuration management plans at both the organizational level and information system level.

3.1.1 PLANNING AT THE ORGANIZATIONAL LEVEL

The following subsections describe the Planning phase activities that are normally conducted by organization-wide security programs. The subsections are listed in the order in which the planning activities typically occur. As always, organizations have flexibility in determining which activities are performed at what level and in what order. Planning at the organizational level should result in an established SCM program with documented policies and procedures that provide direction and support for managing configurations of individual information systems within the organization.

Establish Organization-wide SCM Program

The practice of SCM for ensuring adequate security and facilitating the management of risk within an information environment is most effectively realized if it is implemented in a consistent manner across the organization. Some SCM activities are more effective when performed centrally and typically assigned the responsibility of the organization-wide SCM program.

For organizations with varied and complex information environments, implementing SCM in a consistent and uniform manner across the organization will require coordination of resources at the executive level. A senior management-level program manager should be designated to lead and oversee the organization-wide SCM program. For many large organizations, additional full or part-time staff may also be needed. For smaller organizations, or those with funding or resource constraints, the organization-wide SCM program may be implemented by senior management-level staff that meet as a group to determine the SCM-related activities that will be centrally managed, develop the organization-wide policies and procedures, etc. When an SCM program is initialized at an organization, the SCM program manager should seek to leverage existing configuration management processes that may already be established within the organization. In most cases, responsibilities for management of the SCM program will likely fall on the existing SAISO office.

The SCM program manager should provide knowledge and direction in the form of policies and procedures, communications, training, defined roles and responsibilities, support, and oversight of SCM stakeholders. An organization-wide SCM program also demonstrates management commitment for the effort. This commitment from the top of the organization is communicated throughout the organization down to the individual IS owners.

The SCM program manager should facilitate communications regarding SCM policies, procedures, issues, etc., within the organization. Consideration should be given to a security information management console or “dashboard” to communicate basic project and operational information to SCM stakeholders in language they understand. The SCM program manager should also consider other vehicles for communication such as Web site updates, emails, and newsletters to share milestones, measures of value, and other SCM-related news with SCM stakeholders.

Develop Organizational SCM Policy

The organization is typically responsible for defining documented policies for the SCM program. The SCM program manager develops, disseminates, and periodically reviews and updates the SCM policies for the organization. The policies should be included as a part of the organization-wide security policy. The SCM policy normally includes the following:

- Purpose – the objective(s) in establishing SCM policy;
- Scope – the extent of the information environment to which the policy applies;
- Roles – the roles that are significant within the context of the policy;
- Responsibilities – the responsibilities of each identified role;
- Activities – the functions that must be performed to meet policy objectives;
- Monitoring – the method of verification of policy compliance; and
- Standards – federal and/or organization-wide standards for configuration settings along with exception handling.

SCM policy may also address the following topics:

- SCM training requirements;
- Use of SCM templates;
- Use of automated tools;
- Prohibited configuration settings; and
- Requirements for inventory of information systems and components.

The SCM policy should emphasize management commitment, clarify the required level of coordination among organizational entities, and the monitoring approach.

If the organization has existing policy regarding configuration management of information systems and components, the SCM policy should be integrated into the existing CM policy.

The SAISO or equivalent role is typically responsible for the development of appropriate SCM policy for the organization.

Develop SCM Procedures

The organization typically establishes and maintains common procedures for security configuration management activities; however, some or all SCM procedures may require development at the system level. Organizations may also provide hybrid procedures, i.e., the organization establishes procedures that contain parameters to be defined at the system level. In any case, the procedures should be documented, known, and available to relevant staff, and in compliance with organizational policy. SCM procedures should address the following, as applicable:

SCM Templates - Provides templates related to SCM that integrate the organization-wide SCM policy and procedures and allow individual system owners to fill in information specific to their information system. Templates may be developed for an SCM Plan, system-specific procedure(s), change requests, reporting on SCM, etc. Templates may also be developed to apply specifically to low, moderate, or high-impact information systems.[15] Sample templates are provided in Appendices D and E.

IS Component Inventory – Describes how components are to be managed within the inventory throughout the SDLC (e.g., how new components are added to the inventory, what information about each component is tracked, and how updates are made including removal of retired components). If automated tools are to be used, factors such as how often they will run, who will administer them, who will have access, and how they will be audited should be described.

Baseline Configuration – Identifies the steps for creation of a baseline configuration, content of the baseline configuration, approval of the initial baseline configuration, maintenance of the baseline configuration (i.e., when it should be updated and by whom), and control of the baseline configuration. If applicable, requirements from higher regulatory bodies should be considered and integrated when defining baseline configurations (e.g., requirements from OMB memos, laws such as HIPAA, etc.).

Secure Configuration Standards – Identifies secure configuration settings to be applied to configuration items. The secure configuration standards specified in the procedure should be derived from federal, organizational, or industry standards that are already established (e.g., FDCC, NIST checklists, DISA STIGS, CIS Benchmarks, etc.). Handling of exceptions to the standards should also be addressed (i.e., identification of acceptable methods for assessing, approving, documenting, and justifying deviations to secure configuration standards in the event that the configuration for a given system must diverge from the defined standards due to mission requirements or other constraints.).

Patch Management – Defines how an organization's patch management process is integrated into SCM, how patches are prioritized and approved through the configuration change control process, and how patches are tested for their impact on existing secure configurations. Also defines how patches are integrated into updates to approved baseline configurations and how patch implementation is controlled (access controls, etc.).

[15] Information systems categorized in accordance with FIPS 199, *Standards for Categorization of Federal Information and Information Systems*, and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems.*

Configuration Change Control – Identifies the steps to move a configuration change from its initial request to eventual release into the operational environment. The procedure should include:

- Change request and approval procedures;
- Criteria to determine the types of changes that are configuration-controlled (e.g., specific criteria in the form of a checklist, or a list of configuration changes that are preapproved such as updating antivirus signatures, creating or deleting users, changing defective peripherals, motherboard or hard drives, etc.). Also see Section 3.1.4;
- Security impact analysis procedures;
- Criteria to determine when a change is significant enough to trigger system reauthorization activities;
- Establishment of a group that approves changes (e.g., a Change Control Board);
- Requirements for testing of changes for submission to the CCB;
- Requirements for testing of changes prior to release into the operational environment;
- Requirements for access restrictions for change (i.e., who can make change to the information system and under what circumstances);
- Requirements for rollback of changes in the event that problems occur; and
- Requirements for management of unscheduled changes (e.g., changes needed for critical flaw remediation) that are tailored to support expedited reviews and approvals.

Help Desk Procedures – Describes how change requests originating through the help desk are recorded, submitted, tracked, and integrated into the SCM configuration change control process.

SDLC Procedures – Describes how SCM is used to manage and control system configurations and changes within the organizationally defined SDLC process and throughout the life cycle of a system.

Monitoring – Describes how monitoring activities and related reports are applied to assess the security state of the information system, and how to identify configuration drift (and unauthorized change) within an information system through analysis of monitoring and reporting activities.

Media Library Procedures – Describes management of the media library and should include naming conventions for media, labeling procedures (name/version, date created, retention period, owner, date for destruction, impact or classification level), tracking media, access controls, protections for media integrity (e.g., checksums), inventory checks, capacity planning, and archiving of media.

If SCM procedures are established at the organizational level, the SAISO or equivalent role typically has oversight of this activity. Otherwise, the information system owner determines the procedures required for the information system to comply with organizational SCM policy. Both organizations and system owners have responsibility in determining which procedures are needed and how they should be documented (e.g., as several separate procedures, as a single procedure, as part of the SCM plan).

Determine the Types of Changes Requiring Configuration Change Control

Organizations should determine the types of security related changes to the information system that are configuration-controlled. Information systems are constantly undergoing changes as the mission functions they support are performed. For example, a database-driven portal application is constantly updating the content of the database in servers; administrators are creating new accounts for users within a system; users on a network are creating and deleting user files. It is important to recognize the changes that impact the secure configuration of the information system and differentiate them from changes (such as the examples above) that do not affect the configuration of the information system. The organization may wish to create a list of typical security related changes that do not require configuration control (i.e., changes that are exempt from SCM), as well as a list of changes that should be configuration controlled. Some examples of changes that could require security configuration control are installation of a new operating system on a server, the addition of a new type of component to the system, or the installation of a new/updated application or application module within the system.

Information system owners need to recognize the changes that would represent an update to the secure baseline configuration for the system. These types of changes should be controlled through the configuration change control processes defined by the organization and/or adopted by the information system.

Develop SCM Training

SCM is a fundamental part of an organizational security program but often requires a change in organizational culture. SCM training is more than an opportunity to learn how to maintain baseline configurations; it can facilitate the change in culture and provide a venue for management to communicate the reasons why SCM is important.

The SCM program manager may wish to develop SCM training material covering common organizational policies, procedures, tools, artifacts, and monitoring requirements. The training may be mandatory or optional and should be targeted to relevant staff (e.g., system administrators, system developers, system security officers, system owners, etc.).

If SCM training is developed at the organizational level, the SAISO or equivalent role typically has oversight of this activity. Otherwise, the information system owner determines what training is required to ensure staff have the skills to manage the baseline configurations to comply with organizational SCM policy.

Identify Approved IT Products

Many organizations establish a list of approved hardware and software products for use across the organization. Information system owners are able to select and use products from the approved list without the need for explicit approval. Depending upon organizational policy, additional products required for a particular information system may need to be approved by the CCB for that information system; alternatively, a product used may need to be added to the organizationally controlled and approved IT products list. Some organizations may also provide a buying service or similar purchasing/contracting vehicle from which preapproved products may be purchased or must only be purchased.

If approved IT product lists are established at the organizational level, the SAISO or equivalent role typically has oversight of this activity. Otherwise, the CCB for the information system has the responsibility of approving IT products for that information system.

Identify SCM Tools

In most cases, tools to support SCM activities are selected for use across the organization by SCM program management, and information system owners are responsible for applying the tools to the SCM activities performed on each information system. Similarly, tools and mechanisms for inventory reporting and management may be provided to information system owners from the organizational level. In accordance with federal government and organizational policy, if automated tools are used for SCM, the tools should be Security Content Automation Protocol (SCAP)-validated to the extent that such tools are available. SCAP is described in more detail in Section 3.5.

If not mandated by the organization, tools should be identified and deployed to support SCM at the information system level. When possible, existing SCM tools from within the organization should be leveraged to support consistent organization-wide SCM practices, centralized reporting, and improved cost savings. Leveraging existing tools requires them to be installed and configured to work in the local information system. This usually requires that accounts be set up, administrators identified, schedules for scans determined, the appropriate baseline configurations set up, and possibly installation of a client on each component to be tracked. If the tool has already been deployed within the organization, instructions for installing, configuring, and deploying the product should be available or easy to produce if needed.

In many cases, organizations may want to consider an all-in-one SCM solution for configuration management. For example, various configuration management functions are included in products for managing IT servers, workstations, desktops, and services provided by applications. These products may include functions such as:

- Inventory/discovery of IS components;
- Software distribution;
- Patch management;
- Operating system deployment;
- Policy/secure configuration management;
- Configuration settings migration; and
- Backup/Recovery.

If SCM tools are identified and managed at the organizational level, the SAISO or equivalent role typically has oversight of this activity. Otherwise, the CCB for the information system has the responsibility of approving SCM tools for that information system.

Establish Configuration Test Program

Some organizations may wish to establish and maintain a configuration test environment for centralized testing of IT products. The test environment is used for various types of testing to include:

- IT products proposed for approval and use within the organization;
- Secure configuration settings for approved IT products;
- Patches issued by suppliers prior to their rollout through the organization;
- Validation of SCM tools to detect unapproved configuration settings;
- Verification of testing processes to validate authorized configuration settings; and
- Other configuration-related changes.

NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, provides a set of guidelines on how to establish and conduct an effective information security functional testing program. Specific guidelines are provided for system configuration review and vulnerability scanning which may be directly applied to the configuration test program.

If the organization has established a configuration test program, the SAISO or equivalent role typically has oversight of this activity. Otherwise, the information system owner is responsible for ensuring that products and changes are tested prior to implementation.

3.1.2 PLANNING AT THE SYSTEM LEVEL

The following subsections describe the planning phase activities that are normally completed at the system level. The subsections are listed in the order in which the planning activities typically occur. As always, organizations have flexibility in determining which activities are performed at the organizational level and which activities are performed at the system level, and in what order. The system-level planning phase should result in a completed SCM Plan, an established Change Control Board, an accurate information system component inventory, and defined configuration items for the system.

Develop SCM Plan for Information System

The primary goal of the SCM Plan is to document or provide references to system-specific SCM-related information. The organization may define a master SCM Plan and provide templates that include the typical elements requiring each information system to document a subset of SCM Plan elements that pertain to the particular information system, or the system owner may be required to define the system SCM Plan in its entirety. Regardless of form, factor, or format, a SCM Plan is completed at the system level and typically covers the following topics:

- Brief description of the target information system(s);
- Information system component inventory;
- Information system configuration items;
- Rigor to be applied to managing changes to configuration items (i.e., based on the impact level of the information system[16]);
- Identification of the roles and responsibilities;
- Identification and composition of the group or individual(s) that consider change requests;
- Configuration change control procedures to be followed (including references to organization-wide procedures);
- Identification of the location where SCM artifacts (change requests, approvals, etc.) are maintained (e.g., media libraries);
- Overrides of location of SCM artifacts (if applicable);
- Access controls employed to control changes to configurations;
- Overrides of configuration change control procedures (if applicable);
- SCM tools that are used;
- Description of secure configuration standards (e.g., FDCC, DISA STIGs, NIST checklists, etc.) to be used as basis for establishing approved configuration baselines for the information system;
- Deviations from secure configuration standards for configuration items including justifications; and
- Description of approved baseline configurations for the information system.

[16] Information systems categorized in accordance with FIPS 199, *Standards for Categorization of Federal Information and Information Systems*, and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems.*

The SCM Plan may have various representations; it could be an actual document, a collection of data stored within an SCM tool, or a variety of other representations. The SCM Plan may also be instantiated at the system level from organization templates through SCM procedures.

The IS owner in coordination with the ISSO has the responsibility of developing an SCM Plan/Procedures for an information system.

Create or Update Information System Component Inventory List

An information system component has a physical representation and is equivalent to an IT asset belonging to the organization. An up to date and accurate IS component inventory is an essential mechanism to record the IS components that compose the information system(s) within the organization. The IS component inventory helps to improve the security of the information system by providing a comprehensive view of the IS components that need to be managed and secured. All information system components should be tracked from acquisition to retirement as part of the organization's SDLC process.

The information system component inventory can be represented as:

$$\text{IS Component Inventory} = \{ISC_1, ISC_2, \ldots ISC_n\},$$

where n is greater than or equal to one, and ISC represents an information system component within the organization.

Every IS component within an organization should be included within the authorization boundary of a single information system and should be documented and tracked in an inventory which reflects the association with the information system under which it is managed. An IS component may support information systems that are not within the same authorization boundary (such as a server that supports several Web applications or virtual machines); however, the owners of the supported information systems have neither authority over, nor responsibility for, the supporting component.

The IS component inventory is often populated through a process of discovery. Discovery, which may be manual or automated, is the process of seeking out and recording information on IS components that compose the information systems within the organization. The organization typically determines the types and granularity of the components (peripherals versus workstations, routers, etc.) that are to be identified within the inventory. In most organizations, it is usually impractical to manually collect this information for inclusion in the inventory or for analysis against the authorized inventory. The use of automated tools for discovery, analysis, and management of IS component inventories is generally a more effective and efficient means of maintaining IS component inventories. Further, specifying components by a commonly recognized identifier such as the Common Platform Enumeration (CPE) can facilitate interchange of data among SCAP-compliant tools. Using CPE identifiers from the start of the procurement process would provide a single data source for the IS component inventory to track components from procurement to retirement.

Tools that support inventory management are usually database-driven applications to track and manage information system components within a given environment. Once an inventory is established, automated tools are often used to detect the removal or addition of components. An inventory management tool provides significant value to the SCM process when the inventory data can be correlated with the information systems within the organization. Some inventory management tools allow for expanded monitoring of components through the use of built-in hooks in the OS, installation of agents on each IS component, or Application Protocol Interfaces. With this added functionality, the inventory management system can monitor changes in the component's configuration and report the results to specified staff. When purchasing a Commercial Off-the-Shelf (COTS) or customized inventory management application, organizations would be well advised to include such specific SCAP requirements in requests for proposals, purchase agreements, contracts, etc. If available, inventory management tools should be SCAP validated.

An IS component inventory adds real value to SCM when each item in the inventory is associated with information that can be leveraged for determination of approved secure configuration baselines, configuration change control/security impact analysis, and monitoring/reporting. Some attributes which are typically stored for each item in the IS component inventory include:

- Unique Identifier and/or Serial Number;
- Information System of which the component is a part;
- Type of IS component (e.g., server, desktop, application);
- Manufacturer/Model information;
- Operating System Type and Version/Service Pack Level;
- Presence of virtual machines;*
- Application Software Version/License information;
- Physical location (e.g., building/room number);
- Logical location (e.g., IP address);
- Media Access Control (MAC) address;
- Owner;
- Operational status;
- Primary and secondary administrators; and
- Primary user (if applicable).

Some additional data elements may also be recorded to facilitate SCM, such as:

- Relationships to other IS components in the inventory;*
- Relationships to/dependencies on other information systems;*
- Other information systems supported by this component;*
- Service-Level Agreements (SLA);
- Applicable secure configuration standard;
- Control Item (CI) of which it is a part;
- NIST SP 800-53 security controls supported by this component; and
- Incident log.

*A single IS component may support additional information systems. For example, a server in a server farm may host several virtual machines, and each virtual machine in turn may support a Web application. When such a server suffers a service interruption or compromise, the information stored in the component inventory about the uses of that server can assist in the quick identification of the applications that are impacted so that appropriate actions can be taken. Additionally, virtual machines need tracking and secure configurations of their own, thus it is important for overall organizational risk management, as well as for system-level security, to identify virtual machines and include them in the SCM process.

The IS owner in coordination with the ISSO has the responsibility of populating and maintaining the IS component inventory for an information system.

Determine Configuration Items

When implementing security configuration management, the system owner should determine how to best decompose the information system (IS) into one or more configuration items (CIs). CIs may be one or a group of IS components, documents, network diagrams, scripts, custom code, and various other elements that compose the information system and which require configuration management.

An IS can be represented as a set of one or more CIs as follows:

$IS = \{CI_1, CI_2, ...CI_n\}$ where n is greater than or equal to 1.

There is a one-to-many relationship between ISs and CIs. Thus, each IS is composed of one or more CIs; however, each CI is part of one, and only one, IS.

A CI may be composed of one or more IS components (ISCs), one or more non-component (NC) entities (e.g., documentation or software modules), or some combination thereof as indicated in the following formulas:

i. $CI_A = \{ISC_1, ISC_2, ...ISC_n\}$ where n is greater than or equal to one;
ii. $CI_B = \{NC_1, NC_2, ...NC_n\}$ where n is greater than or equal to one; and/or
iii. $CI_C = \{ISC_1, ISC_2, ...ISC_n + NC_1, NC_2, ...NC_n\}$ where n is greater than or equal to one.

For example, an information system with a number of servers using similar technology may be taken together as one CI (as in formula i). All documentation for the system may be included in one CI or each document may be treated as a separate CI (as in formula ii). The custom code or scripts used may be represented as one or more CIs (as in formula ii). Conversely, the system owner may find that it is more expedient to include the servers, custom code/scripts running on the servers, and supporting documentation in a single CI (as in formula iii). When applying formulas i or ii, it is important to note that the rigor of the review and approval of change proposals for one CI (e.g., a CI composed of servers) may be higher than that applied to another CI (e.g., a CI composed of documentation). Furthermore, CIs within the same system may be tracked using different tools.

Every item within the IS component inventory should be associated with one and only one, CI, and hence, be included within the authorization boundary of a single information system.

Each CI should be assigned an unambiguous identifier so that it can be uniquely referenced within SCM processes. Each CI could have a series of approved baseline configurations as it moves through its life cycle and is the target of configuration change control. As the CI moves through its life cycle, the organization should manage version numbers for the CI.

A set of attributes should be maintained for each CI to define and describe the CI to enable it to be rebuilt from scratch. The types of information that should be associated with a CI include:

- The information system of which the CI is a part;
- Logical and/or physical placement within the system;
- Ownership and management information;
- Inventory of IS components that makes up the CI;
- Inventory of software that makes up the CI;

- Inventory of documentation that makes up the CI;
- Version numbers for software, patch levels, and documents;
- Information related to custom software used within the CI;
- IT product or component secure configuration standard; and
- Any other information needed to rebuild or reconstitute the CI.

While decomposing an information system into a number of CIs makes it easier to manage changes within the information system, it is important to note that when one CI within an IS changes, other CIs within the IS may also be affected. Furthermore, approved changes to a CI may result in updates to the system IS component inventory.

Another potential type of configuration item that should be considered, particularly with respect to establishment and maintenance of a configuration test program is a CI for SCM tools and testing processes. Tools and testing processes used to validate deviations from approved information system baseline configurations should be configuration-controlled to ensure that such testing does not provide false positive or false negative results (i.e., subject tools and processes are able to detect unauthorized configuration settings, and are able to successfully recognize approved configuration settings).

The IS owner in coordination with the ISSO has the responsibility of identifying and naming the CI(s) for an information system.

Establish Change Control Board (CCB) for Information System

A CCB or equivalent group should be identified for the review and approval of change request proposals for the information system. The CCB should be established through the creation of a charter which defines the authority and scope of the group and how it should operate. A charter may define the CCB's membership, the roles and responsibilities of its members, and whether it reports to an oversight body like an Executive Steering Committee. A charter also describes the process by which the CCB operates, including how to handle changes and the range of dispositions (approved, not approved, on hold, etc.), evaluation criteria, and the quorum needed to call a vote.

The CCB plays an important role of gatekeeper, deciding which changes may be acted upon and introduced into an information system. The CCB deliberately considers the potential effect of a proposed change on the security state of the information system, and the risk to the organization should the change be implemented. By reviewing each proposed modification, the CCB ensures that there is a disciplined, systematic, and secure approach for introducing change to the information environment. Having a clearly defined process or framework for the evaluation and approval of change requests, including predefined evaluation criteria, helps ensure that each proposed change is evaluated in a consistent and repeatable manner balancing security, business, and technical viewpoints.

Organizational policy may allow flexibility regarding the size and formality of the CCB. Low-impact and/or small, uncomplicated information systems may require less formality; the CCB may comprise as few as two members (typically the system owner and the ISSO.) For high-impact systems and complex moderate impact-systems, the guidelines for configuration change control may include the institution of a CCB that is composed of at least three individuals, at least one of whom is an ISSO or ISSM. Additionally, for high-impact systems, proposed changes may need to be formally submitted to the CCB, and go through formalized reviews and security impact analysis prior to acceptance and approval.

Regardless of the size and formalism of the CCB for an information system, best practices for configuration change control should require that changes to the information system be vetted by at least one authorized individual who is independent of the requestor – in other words, system administrators, developers, etc., should not have the authority to unilaterally propose and approve changes to the configuration of an information system (excluding changes identified in procedures as being exempt from SCM). The vetting activity should be recorded in an artifact that can be archived.

In selecting members of the CCB, an organization should consider choosing individuals who represent a spectrum of stakeholder needs. The viewpoints of individuals representing the system mission, IT in general, and security in particular, end users, customers, vendors, and other third parties may be considered for inclusion in the CCB. Even if some participants do not have a voting role in the CCB, their input may support improved decision making. For example if security-related changes to specific configuration settings are being considered for a product, representatives of the user community should be involved to ensure that such changes do not adversely impact the functionality of the product.

Unless CCBs are managed at the organization level, the IS owner, in coordination with the ISSO, has the responsibility of establishing the CCB and identifying the members of the CCB for an information system. It is also possible that a single CCB may serve a number of information systems, in which case the set of IS owners and ISSOs for all of the participating information systems are responsible for implementing the CCB.

3.2 CONFIGURING TO A SECURE STATE

The following subsections describe the Configuring to a Secure State phase activities. In this phase, the activities are normally completed at the system level following organizational policy, and possibly some organizational procedures. The subsections are listed in the general chronological order in which the configuration activities should occur. As always, organizations have flexibility in determining which activities are performed at what level and in what order. Completion of the Configuring to a Secure State phase should result in implementation of a secure configuration baseline for each information system and constituent CIs, i.e., each established CI should be the target of a documented and approved secure configuration.

3.2.1 ESTABLISH SECURE CONFIGURATIONS

In developing and deploying an information system, secure configurations should be applied to the information system and its constituent CIs. Secure configurations may include:

- Configuration settings (i.e., the set of parameters that can be changed in a hardware or software component of an information system to affect its security posture) including, but not limited to:
    - OS and application features (enabling or disabling depending on the specific feature);
    - Services and ports (e.g., automatic updates, DNS over port 53);
    - Network protocols (e.g., NetBIOS, IPv6) and network interfaces (e.g., Bluetooth, IEEE 802.11, infrared);
    - Methods of remote access (e.g., SSL, VPN, SSH, and IPSEC);

  - Access controls (e.g., controlling permissions to files, directories, registry keys, and user activities such as restricting activities like modifying system logs or installing applications);
  - Management of identifiers/accounts (e.g., changing default account names, determining length of time until inactive accounts are disabled, using unique user names, establishing user groups);
  - Authentication controls (e.g., password length, use of special characters, minimum password age, multifactor authentication/use of tokens);
  - Audit settings (e.g., capturing key events such as failures, logons, permission changes, unsuccessful file access, creation of users & objects, deletion & modification of system files, registry key and kernel changes);
  - System settings (e.g., session timeouts, number of remote connections, session lock, etc.); and
  - Cryptography (e.g., using FIPS 140-2-validated cryptographic protocols and algorithms to protect data in transit and in storage);

- Patch Levels - applying vendor-released patches in response to identified vulnerabilities, including software updates;
- Software Load and Version - using approved, signed software, if supported;
- Endpoint Protection Platforms - safeguards implemented through software to protect end-user machines against attack (e.g., antivirus, antispyware, antiadware, personal firewalls, host-based intrusion detection systems [HIDS]);
- Transport Protocol Protections (e.g., TLS, IPSEC);
- System Architecture - where a component physically and logically resides (e.g., behind a firewall, within a DMZ, on a specific subnet, etc.); and
- Documentation – supporting documents may include technical specification and design documentation, system security documentation, system procedures, etc.

In many cases, organizational policies, in accordance with federal laws, standards, directives, and orders, establish commonly accepted secure configuration standards (e.g., NIST checklists, DISA STIGs, CIS benchmarks) as the source for secure configurations. The secure configuration standards identified in the NIST checklist program[17] should be used whenever possible; deviations should be justified and recorded in documented form (see Section 3.2.2.iii).

If not identified by the organization, the IS owner, in coordination with the ISSO, has the responsibility of establishing secure configurations for an information system. Regardless of the responsible party, the secure configurations should comply with all applicable federal requirements and should be approved in accordance with organizational policy.

3.2.2 IMPLEMENT SECURE CONFIGURATIONS

Implementing secure configurations for IT products is no simple task. There are many IT products, and each has a myriad of possible configuration settings. In addition, organizations have mission and business process needs which may require that IT products be configured in a particular manner. To further complicate matters, for some products, the configuration settings of the underlying platform may need to be modified such that they deviate from the approved secure configuration standards to allow for the functionality required for mission accomplishment.

[17] National Institute of Standards and Technology Special Publication 800-70, *National Checklist Program for IT Products: Guidance for Checklists Users and Developers*, as amended, provides information on the NIST Checklist Program. Also see http://nvd.nist.gov.

Using the secure configuration previously established (see Section 3.2.1) as a starting point, the following structured approach is recommended when implementing the secure configuration:

i. Prioritize Configurations

In the ideal environment, all IT products within an organization would be configured to the most secure state that still provided the functionality required by the organization. However, due to limited resources and other constraints, many organizations may need to prioritize which information systems, IT products, or CIs to target first for secure configuration as they implement SCM.

In prioritizing which information system, IT products, or CIs to target first for secure configuration, organizations should consider the following criteria:

- System impact level – Information systems that are categorized High or Moderate Impact may be a higher priority to the organization.
- Risk assessments – Risk assessments can be used to target information systems, IT products, or CIs most at risk.
- Vulnerability scanning – Vulnerability scans can be used to target information systems, IT products, or CIs that are most vulnerable. The Common Vulnerability Scoring System (CVSS) is a specification within SCAP that provides an open framework for communicating the characteristics of software flaw vulnerabilities and in calculating their relative severity. CVSS scores can be used to help prioritize patching activities.
- Degree of penetration – The degree of penetration represents the frequency with which the same product is deployed within an information technology environment. For example, if an organization uses a specific operating system on 95 percent of its workstations, it may obtain the most immediate value by planning and deploying secure configurations for that operating system. Other IT products or CIs can be targeted afterwards.

ii. Test Configurations

Organizations should fully test secure configurations prior to implementation in the production environment. There are a number of issues that may be encountered when implementing configurations including software compatibility and hardware device driver issues. For example, although the government requires that commercial vendors ensure that their software is compatible with FDCC, there may be legacy applications with special operating requirements that would not function correctly in FDCC environments. Additionally, configuration errors could occur if OS and multiple application configurations are applied to the same component.

Virtual environments are recommended for testing secure configurations as they allow organizations to examine the functional impact on applications without having to configure actual machines. For the FDCC, a set of virtual machines (one for XP and one for Vista)[18] are available for testing. Organizations can install applications in these virtual machines to determine how FDCC settings impact their existing software loads and services.

[18] The virtual machines may be downloaded from http://nvd.nist.gov/fdcc/download_fdcc.cfm.

iii. Resolve Issues and Document Deviations

Testing of secure configurations will likely reveal compatibility issues of one kind or another. These issues need to be examined individually and either resolved or documented as a deviation from, or exception to, the established organizational standard.

In some cases, changing one configuration setting may require changes to another setting, another CI, or another information system. For instance, FDCC specifies strengthened password requirements, which may require a change to existing single sign-on applications. FDCC has a requirement that Windows firewall be on by default. In order that applications function as expected, the firewall policy may need to be revised. When conflicts between applications and secure configurations cannot be resolved, deviations should be documented and approved through the configuration change control process as appropriate. In the case of FDCC, OMB requires that exceptions to the FDCC standard be approved (consult organizational policy for approval requirements).

iv. Document and Approve the Secure Baseline Configuration

The established secure configuration with deviations should be documented in order to support configuration change control/security impact analysis, incident resolution, problem solving, and monitoring activities. When possible, organizations should employ automated tools to keep documentation as up to date and near real-time as possible. Once documented, the established secure configuration with deviations should be approved in accordance with organizationally-defined policy. Once approved, the established secure configuration with deviations becomes the baseline configuration for the information system and its constituent CIs.

The baseline configuration represents the system-specific configuration against which all changes are controlled. The baseline configuration of an information system is represented as the sum total of the secure configurations of its constituent CIs.

Baseline configurations may include, as applicable, information regarding the system architecture, the interconnection of hardware components, secure configuration settings of software components, the software load, supporting documentation, and the elements in a release package. There could be different baseline configurations for each life cycle stage (development, test, staging, production) of the information system.

When possible, organizations should employ automated tools to support the management of baseline configurations. There are a number of solutions which maintain secure configurations for a wide variety of hardware and software products. Some comprehensive SCM solutions integrate the maintenance of baseline configurations with component inventory and monitoring tools.

v. Deploy the Baseline Configurations

Organizations are encouraged to implement secure baseline configurations in a centralized and automated manner using automated configuration management tools, automated scripts, vendor-provided mechanisms, etc.

Media libraries should be used to store, protect, and control the master copies of documented and approved versions of baseline configurations. Media may be the means to store information (paper, tapes, CD/DVDs, USB drives, etc.) or the information itself (e.g., files, software code).

The media library may also include commercially licensed software, custom-developed software, and other artifacts and documents generated throughout the SDLC.

The IS Owner, in coordination with the ISSO, is responsible for ensuring implementation of the established secure configuration and for ensuring documentation and approval of the baseline configuration for the system. The information system administrator is responsible for implementing secure configuration baselines for components of an information system.

3.3 MAINTAINING SECURE STATE

If organizations are to maintain a secure state for their information systems in an environment where technology is continually evolving and the number and seriousness of threats is expanding, changes to systems must be managed and controlled.

The following subsections describe the Maintaining Secure State phase activities. In this phase, the activities are normally implemented at the system level following organizational policy, and possibly some organizational procedures. The subsections are listed in the order in which the configuration activities typically occur. As always, organizations have flexibility in determining which activities are performed at what level and in what order. Completion of the Maintaining Secure State phase should result in implementation of access restrictions for change, and documented configuration change control and security impact analysis processes.

3.3.1 IMPLEMENT ACCESS RESTRICTIONS FOR CHANGE

Access restrictions for change represent the enforcement side of SCM. Configuration change control is a process for funneling changes for an information system through a managed process; however, without access restrictions, there is nothing preventing someone from implementing changes outside the process. Access restrictions are a mechanism to enforce configuration control processes by controlling who has access to the information system and/or its constituent CIs to make changes.

To implement access restrictions for change:

- **i.** Determine the possible types of configuration changes that can be made in the information system including network, operating system, and application layers;
- **ii.** Determine which individuals have privileged access and which of those privileged individuals are authorized to make what types of changes; and
- **iii.** Implement technical mechanisms (e.g., role-based access, file/group permissions, etc.) to ensure that only authorized individuals are able to make the appropriate changes.

The IS owner in coordination with the ISSO typically has the responsibility of implementing adequate access restrictions to ensure that unauthorized changes cannot be made to the information system or its components.

3.3.2 IMPLEMENT THE CONFIGURATION CHANGE CONTROL PROCESS

A well-defined configuration change control process is fundamental to any SCM program. Configuration change control is the process for ensuring that configuration changes to an information system are formally requested, evaluated for their security impact, tested for effectiveness, and approved before they are implemented. Although the process may have different steps and levels of rigor depending on the organization or system, it generally consists of the following components:

- **i.** **Request** the change. This occurs when a change is initially conceived. The request may originate from any number of sources including the end user of the information system, a help desk, or from management. Changes may also originate from vendor-supplied patches, application updates, etc.

- **ii.** **Document** the request for the change. A change is formally entered into the configuration change control process when it is documented. Organizations may use paper-based requests, emails, or automated tools to track change requests, route them based on workflow processes, and allow for electronic acknowledgements/approvals.

- **iii.** **Determine** if the change requires configuration control. Some types of changes may be exempt from configuration change control as defined in the SCM plan and/or procedures. If the change is exempt, note this on the change request and allow the change to be made without further analysis or approval; however, system documentation may still require updating (e.g., the System Security Plan, the baseline configuration, IS component inventory, etc.).

- **iv.** **Analyze** the change for its security impact on the information system (see Section 3.3.3).

- **v.** **Test** the proposed change for security and functional impacts. The impacts of the change should be presented to the CCB.

- **vi.** **Approve** the change. This step is usually performed by the CCB. The CCB may require the implementation of mitigating controls if the change is necessary for mission accomplishment but has a negative impact on the security of the system and organization.

- **vii.** **Implemen**t the change. Once approved, authorized staff should make the change. Stakeholders (e.g., users, management, help desk, etc.) should be notified about the change, especially if the change implementation requires a service interruption or alters the functionality of the information system. In the case of the latter situation, user and help desk training may be required.

- **viii.** **Confirm** that the change was implemented correctly. Configuration change control is not complete and a change request not closed until it has been confirmed that the change was deployed without issues. Although the initial security impact analysis may reveal no impact from the change, an improperly implemented change can cause its own security issues.

When emergency or unscheduled changes must be made and time does not allow for following the established configuration change control process, emergency changes must still be managed and controlled. Organizations should include instructions for handling emergency changes within the configuration change control procedures. Similarly, configuration change control procedures should address flaw remediation to allow rapid but controlled change to fix software errors. Emergency/unscheduled changes should later be reviewed/resolved by the CCB.

If configuration change control procedures have been defined by the organization, the information system owner should interpret the procedures in the context of the target information system, and refine the process to make it practical to perform. These changes to the process may need to be approved by the organizational CCB in accordance with SCM policy.

Information system owners should endeavor to identify all sources of change to make certain that changes requiring configuration control are funneled through the configuration change control process. It is not uncommon to see activities such as deploying or disposing of hardware, making changes to secure configurations, and installing patches occurring outside the configuration change control process even though these activities can have a significant impact on the security of an information system.

It is important that IT operations and maintenance staff who support the information system are active participants in the configuration change control process and are aware of their responsibility for following it. If significant business process reengineering is needed, for example, updating help desk activities or a patch management process, training may be required.

Once the configuration change control process has been communicated and staff trained, management's responsibility is to enforce the process. The process should be comprehensive enough that exceptions are rarely, if ever, necessary.

The system owner is responsible for ensuring that configuration change control processes are implemented. The CCB for an information system is responsible for approval of changes. The ISSO is responsible for analyzing the security implications of the changes. System administrators and users are responsible for following configuration change control processes.

3.3.3 CONDUCT SECURITY IMPACT ANALYSIS

This is one of the most critical steps in the configuration change control process. Organizations spend significant resources developing and maintaining the security state of information systems; failing to properly analyze a change for its security impact can undo this effort and open up the organization to attack. The security impact analysis activity provides the linkage between configuration change control and improved security. The management of changes through a structured process has its own benefits – for instance, increased efficiency. However, it is only when those changes are evaluated for their security impact that the configuration change control process realizes benefits for the security posture of an information system.

Proposed configuration changes must be examined for impact on security, and the mitigation steps that can be taken to reduce any resulting vulnerability. Security impact analysis should be conducted throughout the SDLC such that the impact of changes on security is considered at every phase:[19]

- **Initiation Phase (Before a Change is Deployed)**
  Security impact analysis before a change is deployed is critical in ascertaining whether the change will impact the security state of the information system. The initial security impact analysis should be conducted before the change is approved by the CCB. This way, if there are security concerns with a change, they can be addressed/mitigated before time and energy are spent in building, testing, and/or rolling out the change.

- **Development/Acquisition and Implementation/Assessment Phases**

[19] Organizations should review NIST SPs 800-27 and SP 800-64 for guidance on integrating security into the SDLC.

Security impact analysis is not a one-time event conducted during the initiation phase to support the decisions of the CCB when approving changes. When the change is initially proposed and reviewed, the manner in which it will be built and implemented may not be known, something which can greatly influence the security impact of the change. For instance, for a custom-built component during the design phase, security impact analysis should be performed on technical design documents to ensure that the design considers security best practices, implements the appropriate controls, and would not need to be redeveloped at a later date due to introduced vulnerabilities. Developers should ensure that security is taken into account as they are building the component, and the design should be tested during implementation to confirm that expected controls were implemented and that no new or unexpected vulnerabilities were introduced.

- **Operations and Maintenance Phase (After a Change is Deployed)** – This confirms that the original security impact analysis was correct, and that unexpected vulnerabilities or impacts to security controls not identified in the testing environment have not been introduced.

The process for a security impact analysis consists of the following steps:

i. **Understand the Change -** If the change is being proposed, develop a high-level architecture overview which shows how the change will be implemented. If the change has been initiated, analyze functional and technical design documents to gain insight into the change.

ii. **Identify Vulnerabilities -** If the change involves a COTS hardware or software product, identifying vulnerabilities may require a search of the National Vulnerability Database (NVD),[20] which enumerates vulnerabilities. Organizations can leverage this information to address known issues and remove or mitigate them before they become a concern. If the change involves custom development, a more in-depth analysis of the security impact should be conducted. Although application security is beyond the scope of this publication, suffice it to say that there are many best practices and useful sources of information for how to ensure the security of software code.

iii. **Assess Risks -** Once a vulnerability has been identified, a risk assessment is needed to identify the likelihood of a threat exercising the vulnerability and the impact of such an event. Although vulnerabilities may be identified in changes as they are proposed, built, and tested, the assessed risk may be low enough that the risk can be accepted without remediation. In other cases, the risk may be high enough that the change is not approved, or that safeguards and countermeasures are implemented to reduce the risk.

iv. **Assess Impact on Existing Security Controls -** In addition to assessing the risk from the change, organizations should analyze whether a change will impact existing security controls. For example, the change may involve installation of software that alters the existing secure configuration; or the change itself may cause or require changes to the existing secure configuration. The change may also affect other components that depend on the function or component being changed, either temporarily or permanently. For example, if a database that is used to support auditing controls is being upgraded to the

[20] http://nvd.nist.gov/

latest version, auditing functionality within the system may be halted while the upgrade is being implemented.

v. **Plan Safeguards and Countermeasures -** In cases where risks have been identified, organizations should use the security impact analysis to revise the change or to plan safeguards and countermeasures to reduce the risk. For instance, if the security impact analysis reveals that the proposed change causes a modification to an FDCC setting, plans to rework the change to function within the existing FDCC settings should be initiated. If a change involves new elevated privileges for users, plans to mitigate the additional risk should be made (e.g., submission of requests for higher clearance levels for those users or implementation of stronger access controls).

SCM program management may wish to develop training and guidance for documenting the security implications for proposed changes so that this activity is done consistently and with a certain level of rigor across the organization. Additionally, the guidance may include the criteria for elevating a particular change request at the information system level to a change request that needs to be submitted to the organizational CCB.

The guidance for considering the security implications for change should also include post-implementation review of the information system to confirm that the change was implemented as approved, and that no additional security implications have surfaced as a result of the change.

The ISSO typically has the responsibility of analyzing proposed changes to determine the security implications. Once the change is approved and implemented, the ISSO is responsible for ensuring that the security stance of the information system has not been negatively impacted as a result of the change.

3.3.4 DOCUMENT AND ARCHIVE

Once the change has been analyzed, approved, tested, and implemented, the organization should update supporting documents such as technical designs and baseline configurations, in addition to security-related documentation such as System Security Plans, Risk Assessments, Security Assessment Reports, and Plan of Action & Milestones. In cases where there is high risk or where significant changes have been made, a system reauthorization may be needed.

As changes are made to baseline configurations, the new baseline becomes the current version, and the previous baseline is no longer valid but is retained for historical purposes. If there are issues with a production release, retention of previous versions allows for a rollback or restoration. Additionally, archiving previous baseline configurations is useful for incident response and traceability support during formal audits.

3.4 MONITORING

If an information system is out of sync with the approved secure configurations as defined by the organization’s baseline configurations of system CIs, the System Security Plan, etc., an organization may have a false sense of security and not take actions that would otherwise limit vulnerabilities and protect it from attacks. Monitoring activities offer the organization better visibility into the true state of security for its information systems.

The security state of information systems should be monitored on an ongoing basis to ensure that the information system is being maintained in accordance with policy and approved baseline configurations. Configuration monitoring activities should confirm that the existing configuration is identical to the current approved baseline configuration, that all items in the IS component inventory can be identified in the information system, and, if possible, whether there are any unregistered or unapproved IS components. Unregistered components are often a major threat to security; they often do not have updated patches, are not configured securely, and are not assessed or included in the authorization to operate. For example, if a technician uses a router for testing and then forgets to remove it, or if an employee sets up a wireless access point in some remote office without management consent, the organization may be vulnerable without the organization being aware of it.

3.4.1 ASSESSMENT AND REPORTING

Configuration monitoring is accomplished through assessment and reporting activities. For organizations with a large number of information system components, the only practical solution for configuration monitoring activities is the use of automated solutions. An information system may have thousands of IS components with hundreds of baseline configurations. To manually collect information on the configuration status of all components and assess them against policy and approved baseline configurations is not practical in most cases. Automated tools can also facilitate reporting for Security Information and Event Management consoles that can be accessed by management and/or formatted into other reports on secure configuration status. Note that care should be exercised in collecting and analyzing the results generated by the automated tool to account for any false positives.

Monitoring may be supported by numerous means, including, but not limited to:

- Scanning to discover components not recorded in the inventory. For example, after testing of a new firewall, a technician forgets to remove it from the network. If it is not properly configured, it may provide access to the network for intruders. A scan would identify this network device as not a part of the inventory, enabling the organization to take action.

- Scanning to identify disparities between the documented and authorized baseline configuration and the actual configuration for an information system. For example, a technician rolls out a new patch but forgets to update the baseline configurations of the information systems impacted by the new patch. A scan could identify a difference between the actual environment and the description in the baseline configuration enabling the organization to take action. In another example, a new tool is installed on the workstations of a few end users of the information system. During installation, the tool changes a number of configuration settings in the browser on the users' workstations, exposing them to attack. A scan would identify the change in the workstation configuration, allowing the appropriate individuals to take action.

- Implementation of automated change monitoring tools. Unplanned or unauthorized changes to the system may be an indication that the system is under attack. Automated tools are available which will monitor specified files within the system for changes and alert system staff if an unplanned or unauthorized change occurs.

- Querying audit reports to identify unauthorized change events.

- Running system integrity checks to verify that baseline configurations have not been changed.

When possible, organizations should seek to normalize data to describe their information system in order that the various outputs from monitoring can be combined, correlated, analyzed, and reported in a consistent manner. SCAP provides a common language for describing vulnerabilities, misconfigurations, and products and is an obvious starting point for organizations seeking a consistent way of communicating across the organization regarding the security state of the information environment (see Section 3.5).

The SCM program manager is typically responsible for establishing the strategy and schedule for SCM monitoring and any associated reporting. Scheduled and ad hoc assessments should be included within the strategy. This schedule may coincide with scheduled releases such that assessments are performed before and after deployments. In other cases, the monitoring activities may be aligned with the dates associated with required reporting, or random assessments may be conducted so that IT staff does not become lax in between scheduled assessments.

When inconsistencies are discovered as a result of monitoring activities, the organization may want to take certain remedial actions. Actions taken may be via manual methods or via use of automated tools. Automated tools are preferable since actions are not reliant upon human intervention and are taken immediately once an unauthorized change is identified. Examples of possible actions include:

- Implementing nondestructive remediation actions (e.g., quarantining of unregistered device(s), blocking insecure protocols, etc.);
- Sending an alert with change details to appropriate staff using email;
- Rolling back changes and restoring from backups;
- Updating the inventory to include newly identified components; and
- Updating baseline configurations to represent new configurations.

Changes detected as a result of monitoring activities should be reconciled with approved changes. Specifically, reconciliation should attempt to answer the following:

- Who made the change;
- Whether the change occurred in a scheduled maintenance window;
- Whether the change matches a previously detected and approved change from a staging environment; and
- Whether the change corresponds with an approved change request, help desk ticket, or product release.

Additionally, the results of monitoring activities should be analyzed to determine the reason(s) that an unauthorized change occurred. There are many potential causes for unauthorized changes. They may stem from:

- Accidental or unintentional changes;
- Individuals with malicious intent;
- Individuals who believe SCM processes don’t apply to them;
- Individuals who aren’t aware of the configuration change control process;
- Errors made when changes are implemented; and
- A delay between introducing the change and updating the inventory and baseline configuration for the affected information systems;

Analyzing unauthorized changes identified through monitoring can not only identify vulnerabilities, but can also give organizations insight into any potential systemic problems with how changes are managed. Once organizations are aware of these activities, they can take actions such as reengineering processes, implementing improved access restrictions for change, and providing training on SCM processes.

Finally, monitoring may support the generation of metrics related to SCM activities. Analysis and consolidation of monitoring reports can generate metrics such as the percentage of information systems that are implemented in accordance with their approved baselines, the percentage of IT products that are configured in accordance with the organizationally-defined secure configuration standards, or percentage of information system changes that have been subjected to security impact analyses. Thus, monitoring is a source of metrics for security implementation within the organization.

Results of monitoring should be reported to management as defined by organizational policy. Various types of reporting may be needed to support compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.

Typically, the SAISO is responsible for establishing and overseeing the configuration monitoring activity across the organization and engaging independent verification teams as appropriate to conduct assessment activities. The ISSO is responsible for ensuring that monitoring activities for the information system are performed in accordance with established policy, while the IS Administrator is responsible for generating the configuration monitoring reports required for the system. Note that some SCM tools are role-based and thus allow assessment and reporting to be conducted by the ISSO without the IS Administrator.

3.4.2 TOOLS FOR MONITORING SECURE CONFIGURATIONS

Managing the myriad configurations found within information system components has become an almost impossible task using manual methods like spreadsheets. When possible, organizations should look for automated solutions which, in the long run, can lower costs, enhance efficiency, and improve the reliability of SCM efforts.

There are a wide variety of configuration management tools available to support an organization's SCM program. At a minimum, the organization should consider a tool that can automatically assess configuration settings of IS components within the information environment. An automated tool should be able to scan different information system components (e.g., Web server, database server, network devices, etc.) running different operating systems, identify the current configuration settings, and indicate where they are noncompliant with policy. Such tools import settings from one or more secure configuration specifications such as those provided through SCAP and then allow for tailoring the settings to the organization's information environment. For example, federal agencies are mandated by OMB[21] to utilize SCAP-enabled tools to verify that FDCC settings for Windows-based workstations and laptops are compliant.

Tools that implement or assess configuration settings should be evaluated to determine whether they meet the following requirements:

[21] OMB Memorandum M-07-11*: Implementation of Commonly Accepted Security Configurations for Windows Operating Systems* and OMB Memorandum M-07-18: *Ensuring New Acquisitions Include Common Security Configurations*

- Can pull information from a variety of sources (different type of components, different operating systems, etc.);
- Use open specifications such as XML and SCAP;
- Offer integration into other products including help desk, inventory management, and incident response solutions;
- Support compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and link vulnerabilities to SP 800-53 controls;
- Provide reporting with the ability to tailor output and drill down; and
- Allow for data consolidation into Security Information and Event Management (SIEM) tools and dashboard products.

The SAISO is typically responsible for identifying monitoring tools (if any) that are to be used across the organization. Alternately, if organizational monitoring tools have not been identified, the ISSO, in consult with the information system owner, is responsible for this activity.

3.5 USING SECURITY CONTENT AUTOMATION PROTOCOL (SCAP)[22]

Security Content Automation Protocol (SCAP) is a protocol currently consisting of a suite of six specifications[23] that standardize the format and nomenclature by which security software communicates information about software flaws and security configurations. SCAP can be used for maintaining the security of enterprise systems, such as automatically verifying the installation of patches, checking system security configuration settings, and examining systems for signs of compromise.

To automate secure configuration management and produce assessment evidence for many NIST SP 800-53 controls, federal agencies should use SCAP-enabled tools along with SCAP-expressed checklists. SCAP-expressed checklists should be customized as appropriate to meet specific organizational requirements. SCAP-expressed checklists can map individual system security configuration settings to their corresponding high-level security requirements. For example, mappings are available between Windows XP security configuration settings and the high-level security controls in NIST Special Publication 800-53, which supports compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. These mappings can help demonstrate that the implemented settings adhere to requirements. The mappings are embedded in SCAP-expressed checklists which allow SCAP-enabled tools to automatically generate assessment and compliance evidence. This can provide a substantial savings in effort and cost. If SCAP-enabled tools are not available or are not currently deployed within an organization, organizations should plan ahead by implementing SCAP-expressed checklists for their secure configuration standards in order to be well-positioned when SCAP-enabled tools become available and/or are deployed.

Organizations should encourage security software vendors to incorporate support for Common Vulnerabilities and Exposures (CVE), Common Configuration Enumeration (CCE), and Common Platform Enumeration (CPE) into their products, as well as encourage all software vendors to

[22] National Institute of Standards and Technology Special Publication 800-117, *Guide to Adopting and Using the Security Content Automation Protocol*, May 2009 (Draft), and 800-126, *The Technical Specification for the Security Content Automation Protocol*, November 2009 provide information on the Security Content Automation Protocol. The text on this page was largely taken from NIST SP 800-117, pages ES-1 and ES-2.

[23] Additional SCAP specifications are expected to be added, check http://scap.nist.gov/ for updates.

include CVE and CCE identifiers and CPE product names in their vulnerability and patch advisories.

SCAP VERSION 1.0 COMPONENTS[24]

SCAP Component	Description	Maintaining Organization
Enumerations		
Common Configuration Enumeration (CCE)	Nomenclature and dictionary of system security issues	MITRE Corporation
Common Platform Enumeration (CPE)	Nomenclature and dictionary of product names and versions	MITRE Corporation
Common Vulnerabilities and Exposures (CVE)	Nomenclature and dictionary of security-related software flaws	MITRE Corporation
Vulnerability Measurement and Scoring		
Common Vulnerability Scoring System (CVSS)	Specification for measuring the relative severity of software flaw vulnerabilities	Forum of Incident Response and Security Teams (FIRST)
Expression and Checking Languages		
Extensible Configuration Checklist Description Format (XCCDF)	Language for specifying checklists and reporting checklist results	National Security Agency (NSA) and NIST
Open Vulnerability and Assessment Language (OVAL)	Language for specifying low-level testing procedures used by checklists	MITRE Corporation

[24] Table taken from National Institute of Standards and Technology Special Publication 800-117, *Guide to Adopting and Using the Security Content Automation Protocol*, May 2009 (Draft). Additional SCAP specifications are expected to be added, check http://scap.nist.gov/ for updates.

APPENDIX A

REFERENCES

LAWS, POLICIES, DIRECTIVES, REGULATIONS, MEMORANDA, STANDARDS, AND GUIDELINES

LEGISLATION

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
3. Paperwork Reduction Act (P.L. 104-13), May 1995.

POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA

4. Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *FEA Consolidated Reference Model Document*, Version 2.3, October 2007.
5. Office of Management and Budget, *Federal Segment Architecture Methodology (FSAM)*, January 2009.
6. Office of Management and Budget Memorandum M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, March 2007.
7. Office of Management and Budget Memorandum M-07-18, *Ensuring New Acquisitions Include Common Security Configurations*, June 2007.
8. Office of Management and Budget Memorandum M-08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)*, August 2008.
9. Office of Management and Budget Memorandum M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, August 2009

STANDARDS

10. Committee for National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, June 2006.
11. Institute of Electrical and Electronic Engineers (IEEE) 1042-1987, *Guide to Software Configuration Management.* (http://standards.ieee.org/reading/ieee/std_public/description/se/1042-1987_desc.html)
12. International Organization for Standardization (ISO) 10007:2003, *Quality management systems – Guidelines for configuration management*. (http://www.iso.org/iso/catalogue_detail.htm?csnumber=36644)
13. International Organization for Standardization (ISO) ISO/ IEC 21827:2008 Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model® (SSE-CMM®). (http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=44716)
14. National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001.
15. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
16. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

GUIDELINES

17. National Institute of Standards and Technology Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.
18. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
19. National Institute of Standards and Technology Special Publication 800-21, 2nd Edition, *Guideline for Implementing Cryptography in the Federal Government*, December 2005.
20. National Institute of Standards and Technology Special Publication 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, August 2000.
21. National Institute of Standards and Technology Special Publication 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000.
22. National Institute of Standards and Technology Special Publication 800-27, Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2004.
23. National Institute of Standards and Technology Special Publication 800-28, Version 2, *Guidelines on Active Content and Mobile Code*, March 2008.
24. National Institute of Standards and Technology Special Publication 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001.
25. National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.
26. National Institute of Standards and Technology Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001.
27. National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February e010.
28. National Institute of Standards and Technology Special Publication 800-39 (Second Public Draft), *Managing Risk from Information Systems: An Organizational Perspective*, April 2008.
29. National Institute of Standards and Technology Special Publication 800-40, Version 2.0, *Creating a Patch and Vulnerability Management Program*, November 2005.
30. National Institute of Standards and Technology Special Publication 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy*, September 2009.
31. National Institute of Standards and Technology Special Publication 800-44, Version 2, *Guidelines on Securing Public Web Servers*, September 2007.
32. National Institute of Standards and Technology Special Publication 800-45, Version 2, *Guidelines on Electronic Mail Security*, February 2007.
33. National Institute of Standards and Technology Special Publication 800-46, Revision 1, *Guide to Enterprise Telework and Remote Access Security*, June 2009.
34. National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.
35. National Institute of Standards and Technology Special Publication 800-48, Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, July 2008.
36. National Institute of Standards and Technology Special Publication 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, September 2002.
37. National Institute of Standards and Technology Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, June 2005.

38. National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009.
39. National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, July 2008.
40. National Institute of Standards and Technology Special Publication 800-54, *Border Gateway Protocol Security*, July 2007.
41. National Institute of Standards and Technology Special Publication 800-55, Revision 1, *Performance Measurement Guide for Information Security*, July 2008.
42. National Institute of Standards and Technology Special Publication 800-57, *Recommendation for Key Management*, March 2007.
43. National Institute of Standards and Technology Special Publication 800-57, Part 3, *Recommendation for Key Management Part 3, Application-Specific Key Management Guidance*, December 2009.
44. National Institute of Standards and Technology Special Publication 800-58, *Security Considerations for Voice Over IP Systems*, January 2005.
45. National Institute of Standards and Technology Special Publication 800-63, Revision 1, (Draft), *Electronic Authentication Guidance*, December 2008.
46. National Institute of Standards and Technology Special Publication 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008.
47. National Institute of Standards and Technology Special Publication 800-68 Revision 1, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals*, October 2008.
48. National Institute of Standards and Technology Special Publication 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*, September 2006.
49. National Institute of Standards and Technology Special Publication 800-70, Revision 1 , *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*, September 2009.
50. National Institute of Standards and Technology Special Publication 800-77, *Guide to IPSec VPNs*, December 2005.
51. National Institute of Standards and Technology Special Publication 800-81, Revision 1 (Draft) *Secure Domain Name System (DNS) Deployment Guide*, August 2009.
52. National Institute of Standards and Technology Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security* (Draft), September 2008.
53. National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006.
54. National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007.
55. National Institute of Standards and Technology Special Publication 800-95, *Guide to Secure Web Services*, August 2007.
56. National Institute of Standards and Technology Special Publication 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, February 2007.
57. National Institute of Standards and Technology Special Publication 800-98, *Guidelines for Security Radio Frequency Identification (RFID) Systems*, April 2007.
58. National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.
59. National Institute of Standards and Technology Special Publication 800-107, *Recommendation for Applications Using Approved Hash Algorithms*, February 2009.
60. National Institute of Standards and Technology Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*, November 2007.
61. National Institute of Standards and Technology Special Publication 800-113, *Guide to SSL VPNs*, July 2008.
62. National Institute of Standards and Technology Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*, September 2008.

63. National Institute of Standards and Technology Special Publication 800-117, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP)* (Draft), May 2009
64. National Institute of Standards and Technology Special Publication 800-118, *Guide to Enterprise Password Management* (Draft), April 2009.
65. National Institute of Standards and Technology Special Publication 800-121, *Guide to Bluetooth Security*, September 2008.
66. National Institute of Standards and Technology Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (Draft), January 2009.
67. National Institute of Standards and Technology Special Publication 800-123, *Guide to General Server Security*, July 2008.
68. National Institute of Standards and Technology Special Publication 800-124, *Guidelines on Cell Phone and PDA Security*, October 2008.
69. National Institute of Standards and Technology Special Publication 800-126, Revision 1, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version1.1*, December 2009.

MISCELLANEOUS PUBLICATIONS

70. Capability Maturity Model Integration (CMMI) (http://www.sei.cmu.edu/legacy/scm/).
71. Information Technology Infrastructure Library (ITIL) (http://www.itil-officialsite.com/home/home.asp).

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for security terminology used within Special Publication 800-53. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.

Active Directory

A Microsoft technology which provides centralized management of services such as authentication and group policy across trusted domains of computers.

Adequate Security
[OMB Circular A-130, Appendix III]

Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Agency

See Executive Agency.

Authentication
[FIPS 200]

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authorizing Official

A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Baseline Configuration

A set of specifications for a system, or CI within a system, that has been formally reviewed and agreed on at a point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

Change Control Board

A group of two or more individuals that review proposed change requests and approve/deny as appropriate.

Checksum

A value computed on data to detect error or manipulation during storage or transmission.

Chief Information Officer
[PL 104-106, Sec. 5125(b)]

Agency official responsible for:

(i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency;

(ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and

(iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

Common Configuration Enumeration

A SCAP specification that provides unique, common identifiers for configuration settings found in a wide variety of hardware and software products.

Common Platform Enumeration

A SCAP specification that provides a standard naming convention for operating systems, hardware, and applications for the purpose of providing consistent, easily parsed names that can be shared by multiple parties and solutions to refer to the same specific platform type.[25]

Common Vulnerabilities and Exposures

An SCAP specification that provides unique, common identifiers for flaws in software.

Common Vulnerability Scoring System

An SCAP specification for communicating the characteristics of vulnerabilities and measuring their relative severity.

Component

See Information System Component.

Configuration

The possible conditions in which an information system or system component can be arranged which affect the security posture of the information system.

Configuration Baseline

See Baseline Configuration.

Configuration Control
[CNSSI 4009]

Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.

Configuration Item

An identified part of an information system that is a discrete target of a configuration control process.

Configuration Management

Comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing changing and monitoring the configurations of those products and systems.

Configuration Management Plan

A comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems.

Configuration Settings

The set of parameters that can be changed in hardware, software, and/or firmware that affect the security posture of the information system.

End-point Protection Platform

Safeguards implemented through software to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, antispyware, antiadware, personal firewalls, host-based intrusion detection systems [HIDS], etc.).

Federal Desktop Core Configuration

OMB-mandated set of security configurations for all federal workstation and laptop devices that run either Windows XP or Vista.

[25] The MITRE Corporation maintains the CPE specifications and NIST maintains the official CPE Dictionary. More information on CPE is available at http://cpe.mitre.org/. The Official CPE Dictionary is available at http://nvd.nist.gov/cpe.cfm .

Group Policy Object

A Microsoft technology for providing centralized management of security configurations for computers in an Active Directory environment.

Host Based Intrusion and Prevention System
[SP 800-94]

A program that monitors the characteristics of a single host and the events occurring within that host to identify and stop suspicious activity.

Incident
[FIPS 200]

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Information Environment
[CNSS Inst. 4009]

An aggregate of individuals, organizations, or systems that collect, process, or disseminate information, also included is the information itself.

Information Resources
[44 U.S.C., Sec. 3502]

Information and related resources, such as personnel, equipment, funds, and information technology.

Information Security
[44 U.S.C., Sec. 3542]

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Policy
[CNSS Inst. 4009]

Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Information System
[44 U.S.C., Sec. 3502]

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.]

Information System Administrator

Individual(s) who implements approved secure baseline configurations, incorporates secure configuration settings for IT products, and conducts/assists with configuration monitoring activities as needed.

Information System Component

A discrete physically identifiable IT asset that represents a building block of an information system.

Information System Component Inventory

A list of the physically identifiable IT assets within an information system.

Information System Owner (or Program Manager)

Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information System Security Officer
[CNSS Inst. 4009, Adapted]

Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program.

Information System User

Person who uses the information system functions and initiates change requests and assists with functional testing.

Information Technology
[40 U.S.C., Sec. 1401]

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Information Technology Product

A system, component, application, etc., that is based upon technology which is used to electronically process, store, or transmit information.

Malicious Code

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Malware

See Malicious Code.

Media

Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Media Library

Stores, protects, and controls all authorized versions of media CIs.

Misconfiguration

An improper configuration of an information system or system component that leads to a vulnerability being exposed.

Network-Based Intrusion Detection and Prevention System
[SP 800-94]

An intrusion detection and prevention system that monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify and stop suspicious activity.

Organization
[FIPS 200]

An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).

Remote Access

Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).

Risk Management
[FIPS 200]

The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Safeguards
[CNSS Inst. 4009, Adapted]

Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Secure Configuration Standard

An established benchmark (e.g., NIST checklists, DISA STIGs, etc.) that stipulates specific secure configuration settings for a given IT platform.

Security Configuration Management (SCM)

The management and control of secure configurations for an information system to enable security and the management of risk.

Security Content Automation Protocol (SCAP)

A protocol currently consisting of a suite of six specifications[26] that standardize the format and nomenclature by which security software communicates information about software flaws and security configurations.

Security Controls

[FIPS 199]

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Impact Analysis

The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

Senior Agency Information Security Officer

Individual that provides organization-wide procedures and/or templates for SCM, manages or participates in the Change Control Board, and/or provides technical staff for security impact analyses.

Spam

The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Spyware

Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

System

See Information System.

System Security Plan
[NIST SP 800-18]

Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

[26] Additional SCAP specifications are expected to be added, check http://scap.nist.gov/ for updates.

Threat
[CNSS Inst. 4009, Adapted]

Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat Source
[FIPS 200]

The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.

User
[CNSSI 4009, adapted]

Individual, or (system) process acting on behalf of an individual, authorized to access an information system.

Vulnerability
[CNSS Inst. 4009, Adapted]

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Whitelist
[SP 800-94]

A list of discrete entities, such as hosts or applications that are known to be benign.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

AV	Antivirus
CCB	Change Control Board
CCE	Common Configuration Enumeration
CD	Compact Disc
CFR	Code of Federal Regulations
CGI	Common Gateway Interface
CI	Configuration Item
CIO	Chief Information Officer
CIS	Center for Internet Security
CM	Configuration Management
CMMI	Capability Maturity Model Integration
CNSS	Committee for National Security Systems
COTS	Commercial Off-the-Shelf
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DISA	Defense Information Systems Agency
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name System
DVD	Digital Video Disc
EPP	Endpoint Protection Platform
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
GPO	Group Policy Object
GUI	Graphical User Interface
HIDS	Host-based Intrusion Detection System
IDPS	Intrusion Detection and Prevention System
IS	Information System
ISA	Information System Administrator

ISC	Information System Component
ISO	International Organization for Standardization
ISO	Information System Owner
ISSO	Information System Security Officer
ISSM	Information System Security Manager
ISU	Information System User
IT	Information Technology
ITIL	Information Technology Infrastructure Library
NetBIOS	Network Basic Input/Output System
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NC	Non-component
NSA	National Security Agency
OMB	Office of Management and Budget
PMO	Program Management Office
SAISO	Senior Agency Information Security Officer
SAM	Security Accounts Manager
SCAP	Security Content Automation Program
SCM	Security Configuration Management
SDLC	System Development Life Cycle
SEE-CMM	Systems Security Engineering - Capability Maturity Model®
SIEM	Security Information and Event Management
SLA	Service-Level Agreement
SP	Special Publication
SSH	Secure Shell
SSP	System Security Plan
STIG	Security Technical Implementation Guidelines
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
XML	Extensible Markup Language

APPENDIX D

SAMPLE SECURITY CONFIGURATION MANAGEMENT PLAN

A TEMPLATE

The following outline is a sample template for developing a Configuration Management Plan for an information system. Organizations are encouraged to adapt the template to make it suitable for their operational environment.

1. INTRODUCTION
    - 1.1 BACKGROUND *[Overview of configuration management and its purpose]*
    - 1.2 OVERVIEW OF SYSTEM *[System description; may reference relevant section of System Security Plan]*
        - 1.2.1 System Mission
        - 1.2.2 Data Flow Description
        - 1.2.3 System Architecture
        - 1.2.4 System Administration and Management Activities
    - 1.3 PURPOSE OF THIS DOCUMENT *[Use of this document]*
    - 1.4 SCOPE *[Applicability of this plan]*
    - 1.5 APPLICABLE POLICIES, STANDARDS, AND PROCEDURES *[List of applicable federal and organizational policies, standards, and procedures]*

2. SCM PROGRAM
    - 2.1 SCM ROLES AND RESPONSIBILITIES *[Description of roles/responsibilities of members of CCB]*
    - 2.2 SCM PROGRAM ADMINISTRATION *[Procedures for CCB]*
        - 2.2.1 Change Control Board Functions
        - 2.2.2 Schedules and Resource Requirements
    - 2.3 SCM PROCESSES AND TOOLS *[Tools and Archival locations for CCB]*
        - 2.3.1 SCM Tools
        - 2.3.2 SCM Library
    - 2.4 CI RETENTION, ARCHIVING, STORAGE AND DISPOSAL *[Requirements for managing historical information on CIs]*

3. SCM ACTIVITIES
    - 3.1 CONFIGURATION IDENTIFICATION
        - 3.1.1 Types of Configuration Items (CI) *[Description of categories of CIs, such as HW, Documentation, SW and scripts, Web pages]*
        - 3.1.2 Identification Criteria *[Way to determine which CIs will be tracked as part of this system and which are tracked under other systems]*
        - 3.1.3 Configuration Item Labeling *[Naming convention for CIs]*
    - 3.2 CONFIGURATION BASELINING *[Defining the information to be included in baseline for each type of CI]*
        - 3.2.1 Hardware Baselines
        - 3.2.2 Non-Hardware CI Baselines
    - 3.3 CONFIGURATION CHANGE CONTROL *[Requirements related to change control]*

3.4 SCM MONITORING *[Requirements related to monitoring secure configuration baselines and compliance with SCM policies]*

3.5 SCM REPORTING *[Requirements related to reporting SCM monitoring results and statistics to appropriate organizational staff]*

APPENDIX: SAMPLE CHANGE REQUEST

APPENDIX E

SAMPLE CHANGE REQUEST

A TEMPLATE

The following is a sample template for a Change Request artifact that can be used within an SCM program. Organizations are encouraged to adapt it to suit their needs.

1. **Date Prepared**:
2. **Title of Change Request**:
3. **Change Initiator/Project Manager**:
4. **Change Description**:
5. **Change Justification**:
6. **Urgency of Change**: {Scheduled/Urgent/Unscheduled}
7. **Personnel involved with the Change**:
8. **Expected Security Impact of Change:**
9. **Expected Functional Impact of Change:**
10. **Expected Impact of Not Doing Change**:
11. **Potential Interface/Integration Issues**:
12. **Required Changes to Existing Applications**:
13. **Project work plan including change implementation date, deliverables, and back-out plan**:
14. **Funding Required to Implement Change**:

APPENDIX F

BEST PRACTICES FOR ESTABLISHING SECURE CONFIGURATIONS

Although there is no one-size-fits-all approach to SCM, there are practices that organizations should consider when developing and deploying secure configurations. These include:

1. Use Standards for Secure Configuration Settings.

Organizations should consider available standards as the basis for establishing secure configuration settings. A source for information on configuration settings is the National Checklist Program. These checklists cover a wide range of commercial products and are written in a standardized format to facilitate automatic assessment through SCAP-enabled tools. Note that the FDCC standard is mandatory for federal Windows XP and Vista machines per OMB Memo 08-22.

References:
NIST SP 800-27: *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*;
NIST SP 800-68: *Guide to Securing Microsoft Windows XP Systems for IT Professionals*;
NIST SP 800-69: *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*;
NIST SP 800-70: *National Checklist Program for IT Products-Guidelines for Checklist Users and Developers*; and
NIST SP 800-117: *Guide to Adopting and Using the Security Content Automation Protocol (SCAP)* (Draft); and
http://nvd.nist.gov.

2. Centralize Policy and Standards for Configuration Settings.

Where possible and appropriate, secure configurations should be developed and implemented in a top-down approach to ensure consistency across the organization. An example is the implementation of the group policy functionality, which can be used to distribute secure configuration policy in a centralized manner throughout established domains. Exceptions to the organization's policy may be needed to tailor configurations for a particular information system to support local constraints or requirements. Such exceptions should be documented and approved as a part of the baseline configuration for that information system.

References: None.

3. Tailor Secure Configurations According to System/Component Function and Role.

Secure configuration settings should be tailored to the system component's function. For example, a server acting as a Windows domain controller may require stricter auditing requirements (e.g., auditing successful and unsuccessful account logons) than a file server. A public access Web server in a DMZ may require that fewer services are running than in a Web server behind an organization's firewall supporting an intranet.

References:
NIST SP 800-41: *Guidelines on Firewalls and Firewall Policy*;
NIST SP 800-44: *Guidelines on Securing Public Web Servers*;
NIST SP 800-45: *Guidelines on Electronic Mail Security*;

NIST SP 800-46: *Guide to Enterprise Telework and Remote Access Security*;
NIST SP 800-48: *Guide to Securing Legacy IEEE 802.11 Wireless Networks;*
NIST SP 800-52: *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*;
NIST SP 800-54: *Border Gateway Protocol Security*;
NIST SP 800-58: *Security Considerations for Voice Over IP Systems*;
NIST SP 800-77: *Guide to IPsec VPNs*;
NIST SP 800-81: *Secure Domain Name System (DNS) Deployment Guide*;
NIST SP 800-82: *Guide to Industrial Control Systems (ICS) Security*;
NIST SP 800-92: *Guide to Computer Security Log Management*;
NIST SP 800-95: *Guide to Secure Web Services*;
NIST SP 800-97: *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*;
NIST SP 800-98: *Guidelines for Securing Radio Frequency Identification (RFID) Systems*;
NIST SP 800-113: *Guide to SSL VPNs*;
NIST SP 800-121: *Guide to Bluetooth Security*;
NIST SP 800-123: *Guide to General Server Security*; and
NIST SP 800-124: *Guidelines on Cell Phone and PDA Security*.

4. Eliminate Unnecessary Ports, Services, and Protocols (Least Functionality).

Devices should be configured to allow only the necessary ports, protocols, and services in accordance with functional needs and the risk tolerance in the organization. Open ports and available protocols and services are an inviting target for attackers, especially if there are known vulnerabilities associated with a given port, protocol, or service. Sources such as the NIST National Vulnerability Database (NVD) are available for highlighting vulnerabilities in various system components.

References: http://nvd.nist.gov/.

5. Limit the Use of Remote Connections.

While connecting remotely to information systems allows more flexibility in how users and system administrators accomplish their work, it also opens an avenue of attack popular with hackers. Use of remote connections should be limited to only those absolutely necessary for mission accomplishment.

References:
NIST SP 800-41: *Guidelines on Firewalls and Firewall Policy*;
NIST SP 800-46: *Guide to Enterprise Telework and Remote Access Security*;
NIST SP 800-47: *Security Guide for Interconnecting Information Technology Systems;*
NIST SP 800-52: *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*;
NIST SP 800-54: *Border Gateway Protocol Security*;
NIST SP 800-77: *Guide to IPsec VPNs*;
NIST SP 800-81: *Secure Domain Name System (DNS) Deployment Guide*;
NIST SP 800-95: *Guide to Secure Web Services*; and
NIST SP 800-113: *Guide to SSL VPNs*.

6. Develop Strong Password Policies.

Passwords are a common mechanism for authenticating the identity of users and if they are poorly implemented or used, an attacker can undermine the best security configuration. Organizations should stipulate password policies and related requirements with the strength appropriate for protecting access to the organization's assets.

References:
NIST SP 800-63: *Electronic Authentication Guideline*; and
NIST SP 800-118: *Guide to Enterprise Password Management* (draft).

7. Implement Endpoint Protection Platforms (EPPs)

Personal computers are a fundamental part of any organization's information system. They are an important source of connecting end users to networks and information systems, and are also a major source of vulnerabilities and a frequent target of attackers looking to penetrate a network. User behavior is difficult to control and hard to predict, and user actions, whether it is clicking on a link that executes malware or changing a security setting to improve the usability of their PC, frequently allow exploitation of vulnerabilities. Commercial vendors offer a variety of products to improve security at the "endpoints" of a network. These EPPs include:

a. Anti-malware

Anti-malware applications should be a part of the standard secure configuration for system components. Anti-malware software employs a wide range of signatures and detection schemes, automatically updates signatures, disallows modification by users, run scans on a frequently scheduled basis, have an auto-protect feature set to scan automatically when a user action is performed (e.g., opening or copying a file), and may provide protection from zero-day attacks. For platforms for which anti-malware software is not available, other forms of anti-malware such as rootkit detectors may be employed.

b. Personal Firewalls

Personal firewalls provide a wide range of protection for host machines including restriction on ports and services, control against malicious programs executing on the host, control of removable devices such as USB devices, and auditing and logging capability.

c. Host-based Intrusion Detection and Prevention System (IDPS)

Host-based IDPS is an application that monitors the characteristics of a single host and the events occurring within that host to identify and stop suspicious activity. This is distinguished from network-based IDPS, which is an intrusion detection and prevention system that monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify and stop suspicious activity.

d. Restrict the use of mobile code.

Organizations should be cautious in allowing the use of "mobile code" such as ActiveX, Java, and JavaScript. An attacker can easily attach a script to a URL in a Web page or email that, when clicked, will execute malicious code within the computer's browser.

References:
NIST SP 800-28: *Guidelines on Active Content and Mobile Code*;
NIST SP 800-41: *Guidelines on Firewalls and Firewall Policy*;
NIST SP 800-47: *Security Guide for Interconnecting Information Technology Systems*;
NIST SP 800-54: *Border Gateway Protocol Security*; and
NIST SP 800-94: *Guide to Intrusion Detection and Prevention Systems (IDPS).*

8. Use Cryptography.

In many systems, especially those processing, storing, or transmitting information that is moderate impact or higher for confidentiality, cryptography should be considered as a part of an information system's secure configuration. There are a variety of places to implement cryptography to protect data including individual file encryption, full disk encryption, Virtual Private Network connections, etc.

References:
FIPS 140-2: *Security Requirements for Cryptography Modules*;
NIST SP 800-21: *Guideline for Implementing Cryptography in the Federal Government*;
NIST SP 800-25: *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*;
NIST SP 800-29: *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*;
NIST SP 800-32: *Introduction to Public Key Technology and the Federal PKI Infrastructure*;
NIST SP 800-57 *(parts 1-3): Recommendation for Key Management*;
NIST SP 800-107: *Recommendation for Applications Using Approved Hash Algorithms*; and
NIST SP 800-111: *Guide to Storage Encryption Technologies for End User Devices*.

9. Develop a Patch Management Process.

A robust patch management process is important in reducing vulnerabilities in an information system. As patches greatly impact the secure configuration of an information system, the patch management process should be integrated into SCM at a number of points within the four SCM phases including:

- Performing security impact analysis of patches;
- Testing and approving patches as part of the configuration change control process;
- Updating baseline configurations to include current patch level;
- Assessing patches to ensure they were implemented properly; and
- Monitoring systems/components for current patch status.

References:
NIST SP 800-40: *Creating a Patch and Vulnerability Program.*

10. Control Software Installation.

The installation of software is a point where many vulnerabilities are introduced into an organization's information system. Malware or insecure software can give attackers easy access to an organization’s otherwise tightly protected network. Although the simplest approach is to lock down computers and manage software installation centrally, this is not always a viable option in many organizations. Other methods for controlling the installation of software include:

- Whitelisting – All software is checked against a list approved by the organization;
- Checksums – All software is checked to make sure the code has not changed;
- Certificate – Only software with signed certificates from a trusted vendor is used;
- Path or domain – Only software within a directory or domain can be installed; and
- File extension – Software with certain file extensions such as .bat cannot be installed.

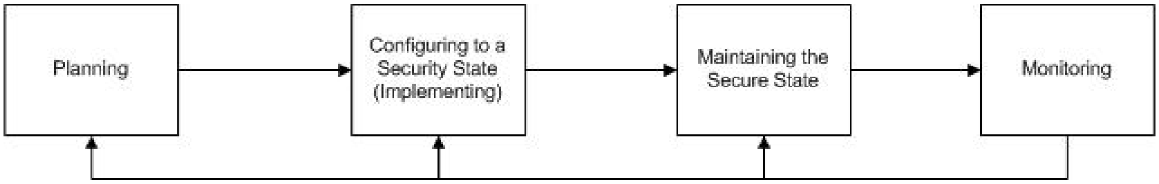
References: None.

APPENDIX G

SCM PROCESS FLOW CHARTS

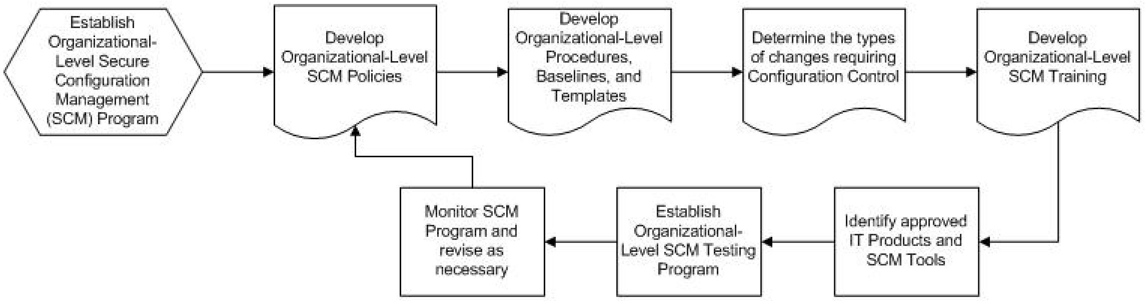
The following flow charts provide examples of the SCM phases and SCM activities for those phases that could be considered in developing SCM processes. Organizations are encouraged to adapt the template to make it suitable for their operating environment.

Secure Configuration Management Phases


Planning
Configuring to a Security State (Implementing)
Maintaining the Secure State
Monitoring

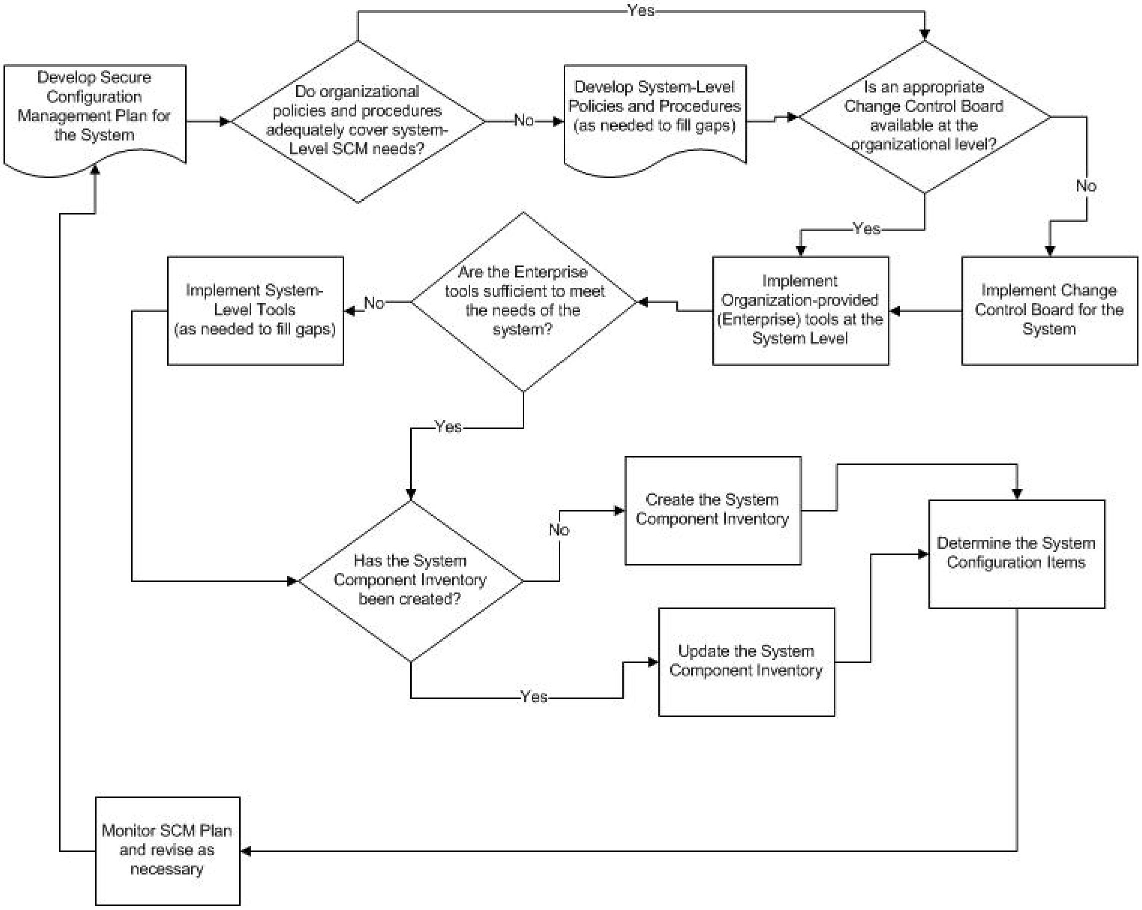
Organizational-Level Secure Configuration Management Program Planning Step Tasks

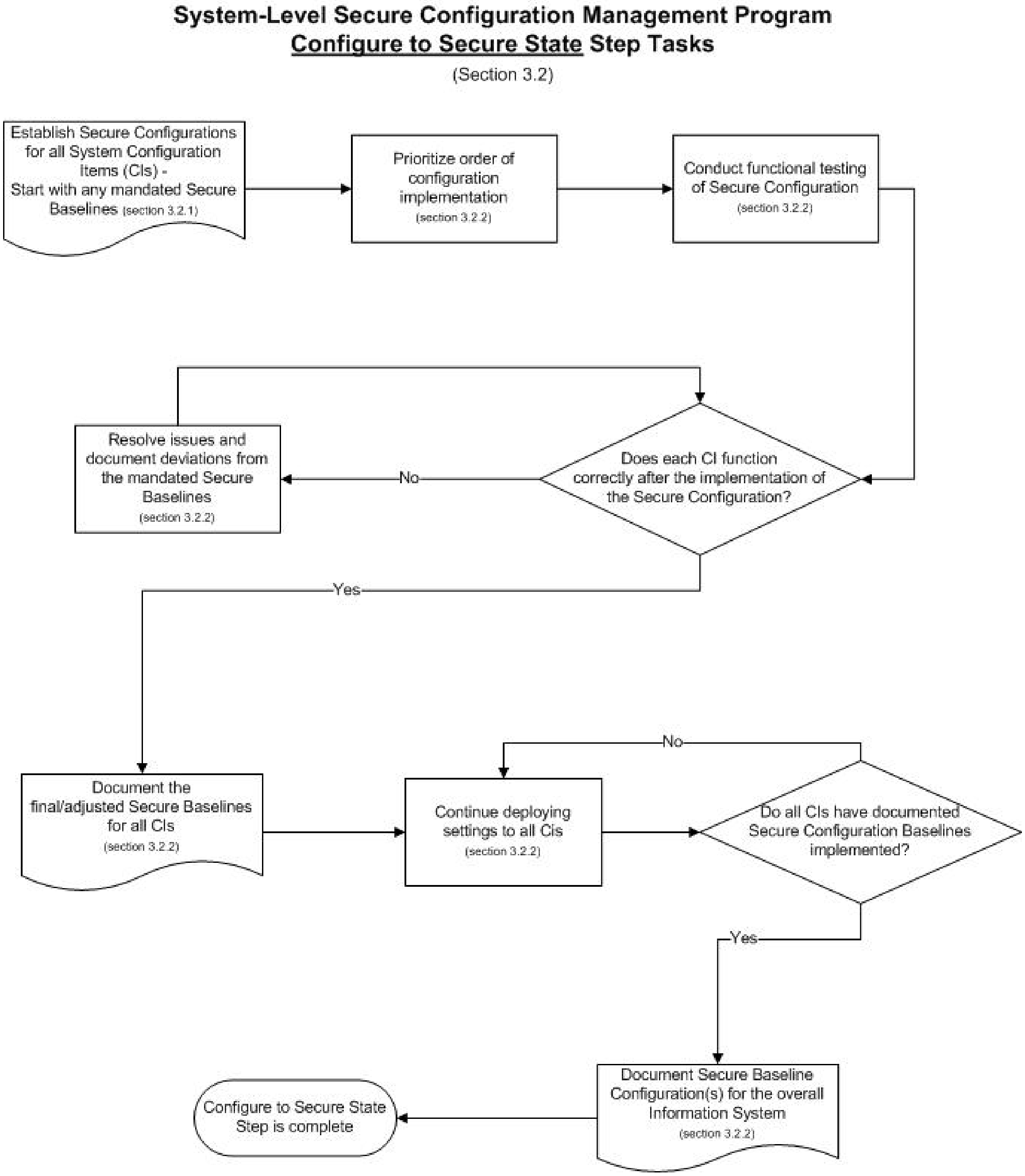
(Section 3.1.1)


Establish Organizational-Level Secure Configuration Management (SCM) Program
Develop Organizational-Level SCM Policies
Develop Organizational-Level Procedures, Baselines, and Templates
Determine the types of changes requiring Configuration Control
Develop Organizational-Level SCM Training
Identify approved IT Products and SCM Tools
Establish Organizational-Level SCM Testing Program
Monitor SCM Program and revise as necessary

System-Level Secure Configuration Management Program Planning Step Tasks

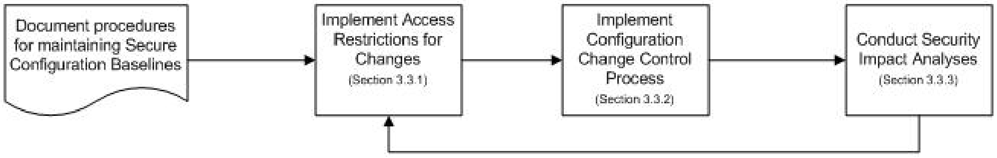
(Section 3.1.2)


Develop Secure Configuration Management Plan for the System
Do organizational policies and procedures adequately cover system-Level SCM needs?
Yes
No
Develop System-Level Policies and Procedures (as needed to fill gaps)
Is an appropriate Change Control Board available at the organizational level?
Yes
No
Implement Change Control Board for the System
Implement Organization-provided (Enterprise) tools at the System Level
Are the Enterprise tools sufficient to meet the needs of the system?
No
Implement System-Level Tools (as needed to fill gaps)
Yes
Has the System Component Inventory been created?
No
Create the System Component Inventory
Yes
Update the System Component Inventory
Determine the System Configuration Items
Monitor SCM Plan and revise as necessary


System-Level Secure Configuration Management Program
Configure to Secure State Step Tasks
(Section 3.2)
Establish Secure Configurations for all System Configuration Items (CIs) - Start with any mandated Secure Baselines (section 3.2.1)
Prioritize order of configuration implementation (section 3.2.2)
Conduct functional testing of Secure Configuration (section 3.2.2)
Does each CI function correctly after the implementation of the Secure Configuration?
No
Resolve issues and document deviations from the mandated Secure Baselines (section 3.2.2)
Yes
Document the final/adjusted Secure Baselines for all CIs (section 3.2.2)
Continue deploying settings to all Cis (section 3.2.2)
Do all CIs have documented Secure Configuration Baselines implemented?
No
Yes
Document Secure Baseline Configuration(s) for the overall Information System (section 3.2.2)
Configure to Secure State Step is complete

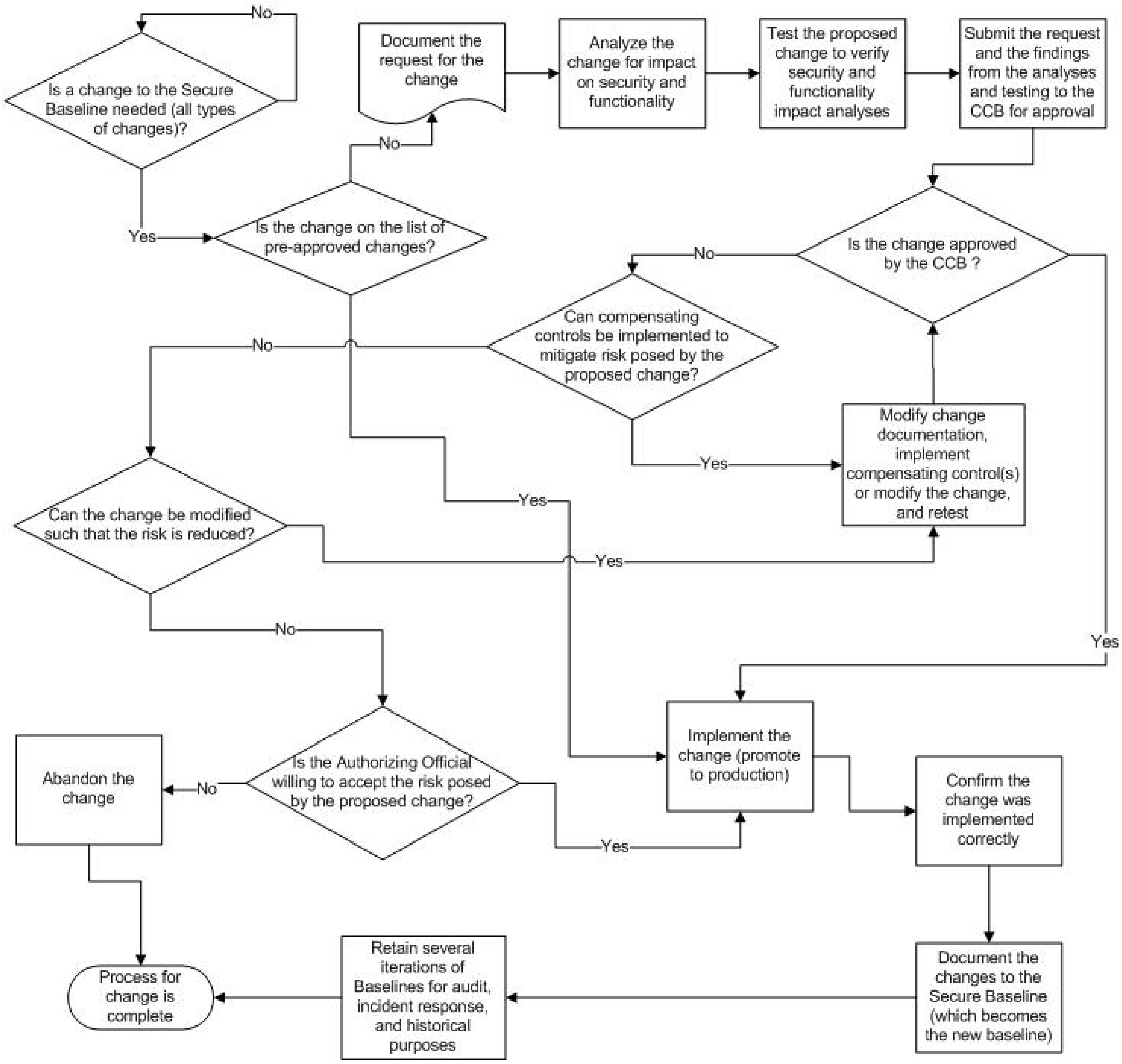
System-Level Secure Configuration Management Program Maintaining the Secure State Step Tasks

(Section 3.3)


Document procedures for maintaining Secure Configuration Baselines
Implement Access Restrictions for Changes (Section 3.3.1)
Implement Configuration Change Control Process (Section 3.3.2)
Conduct Security Impact Analyses (Section 3.3.3)

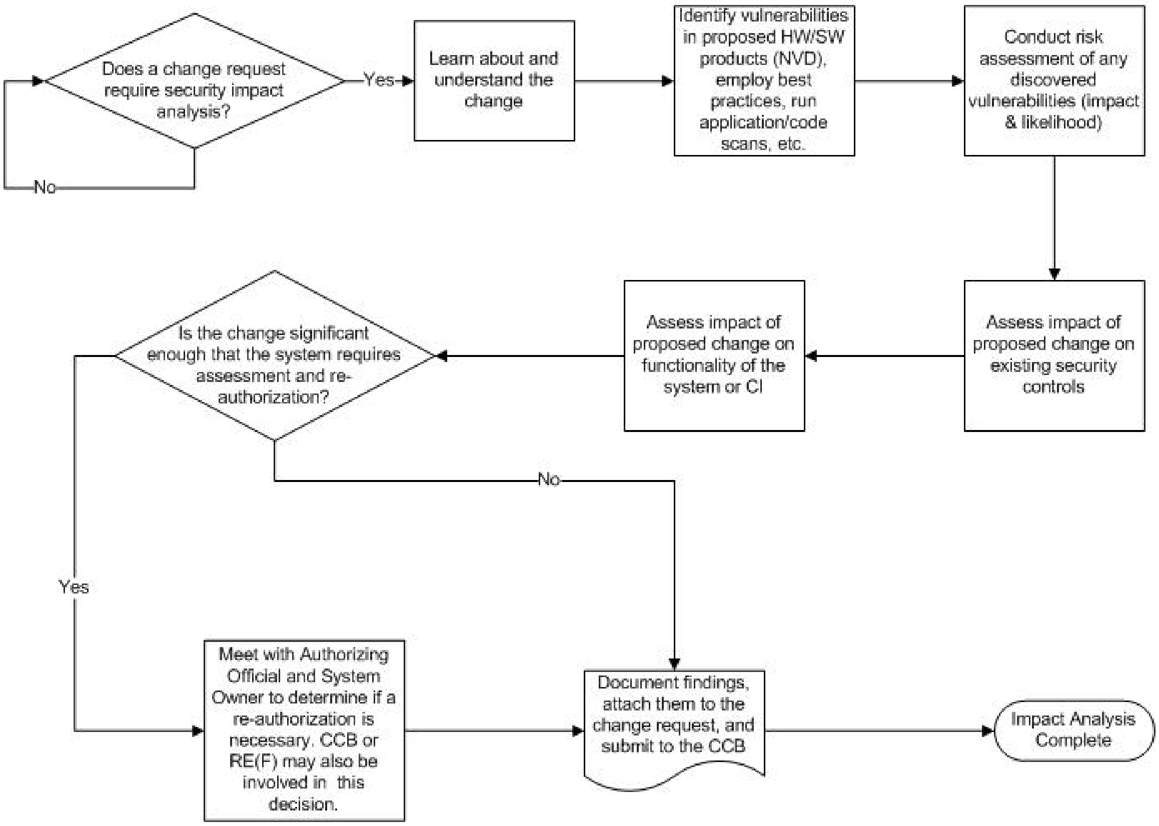
Maintaining the Secure State – Implement Configuration Change Control Process

(Section 3.3.2)


Is a change to the Secure Baseline needed (all types of changes)?
No
Yes
Document the request for the change
Analyze the change for impact on security and functionality
Test the proposed change to verify security and functionality impact analyses
Submit the request and the findings from the analyses and testing to the CCB for approval
Is the change on the list of pre-approved changes?
No
Is the change approved by the CCB ?
No
Yes
Can compensating controls be implemented to mitigate risk posed by the proposed change?
No
Yes
Modify change documentation, implement compensating control(s) or modify the change, and retest
Can the change be modified such that the risk is reduced?
Yes
Yes
No
Is the Authorizing Official willing to accept the risk posed by the proposed change?
No
Yes
Abandon the change
Implement the change (promote to production)
Confirm the change was implemented correctly
Document the changes to the Secure Baseline (which becomes the new baseline)
Retain several iterations of Baselines for audit, incident response, and historical purposes
Process for change is complete

Maintaining the Secure State – Conduct Security Impact Analyses

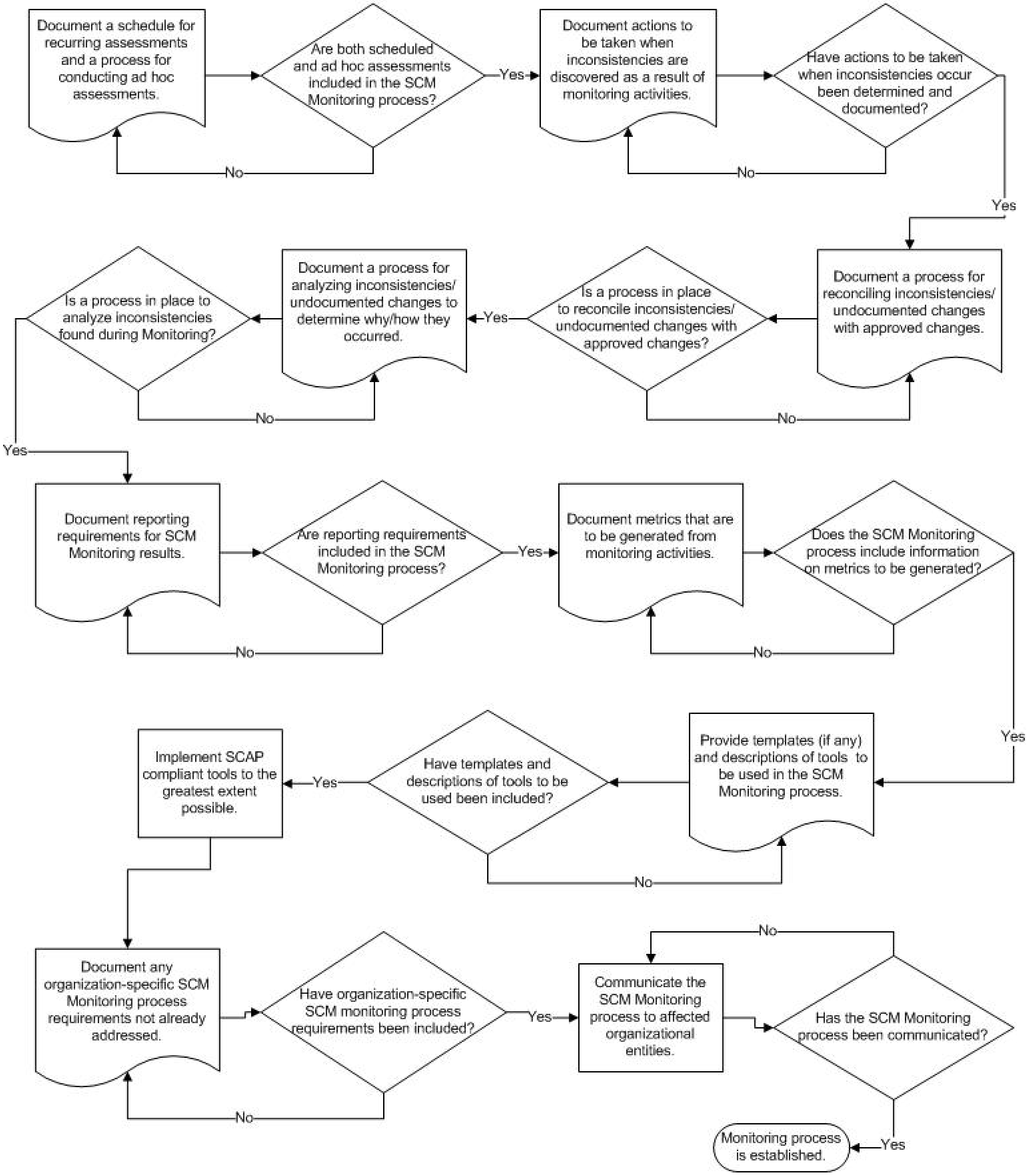
(Section 3.3.3)


Does a change request require security impact analysis?
Yes
No
Learn about and understand the change
Identify vulnerabilities in proposed HW/SW products (NVD), employ best practices, run application/code scans, etc.
Conduct risk assessment of any discovered vulnerabilities (impact & likelihood)
Assess impact of proposed change on existing security controls
Assess impact of proposed change on functionality of the system or CI
Is the change significant enough that the system requires assessment and re-authorization?
No
Yes
Meet with Authorizing Official and System Owner to determine if a re-authorization is necessary. CCB or RE(F) may also be involved in this decision.
Document findings, attach them to the change request, and submit to the CCB
Impact Analysis Complete

Organizational-Level Secure Configuration Management Program Monitoring Step

Establish the SCM Monitoring Process

(Section 3.4)


Document a schedule for recurring assessments and a process for conducting ad hoc assessments.
Are both scheduled and ad hoc assessments included in the SCM Monitoring process?
Yes
No
Document actions to be taken when inconsistencies are discovered as a result of monitoring activities.
Have actions to be taken when inconsistencies occur been determined and documented?
No
Yes
Document a process for reconciling inconsistencies/ undocumented changes with approved changes.
Is a process in place to reconcile inconsistencies/ undocumented changes with approved changes?
No
Yes
Document a process for analyzing inconsistencies/ undocumented changes to determine why/how they occurred.
Is a process in place to analyze inconsistencies found during Monitoring?
No
Yes
Document reporting requirements for SCM Monitoring results.
Are reporting requirements included in the SCM Monitoring process?
No
Yes
Document metrics that are to be generated from monitoring activities.
Does the SCM Monitoring process include information on metrics to be generated?
No
Yes
Provide templates (if any) and descriptions of tools to be used in the SCM Monitoring process.
Have templates and descriptions of tools to be used been included?
No
Yes
Implement SCAP compliant tools to the greatest extent possible.
Document any organization-specific SCM Monitoring process requirements not already addressed.
Have organization-specific SCM monitoring process requirements been included?
No
Yes
Communicate the SCM Monitoring process to affected organizational entities.
Has the SCM Monitoring process been communicated?
No
Yes
Monitoring process is established.